

65933-049
KUNISA
November 3, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 8 日
Date of Application:

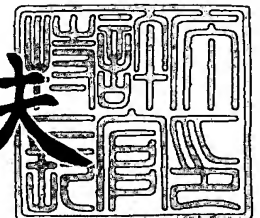
出 願 番 号 特 願 2 0 0 2 - 3 2 5 8 9 6
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 2 5 8 9 6]

出 願 人 三 洋 電 機 株 式 会 社
Applicant(s):

2 0 0 3 年 1 0 月 1 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 8 5 8 5 8

【書類名】 特許願

【整理番号】 NQR1020018

【提出日】 平成14年11月 8日

【あて先】 特許庁長官殿

【国際特許分類】 G06T 1/00
G09C 5/00
H04N 1/387

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社
社内

【氏名】 国狭 亜輝臣

【特許出願人】

【識別番号】 000001889

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100105924

【弁理士】

【氏名又は名称】 森下 賢樹

【電話番号】 03-3461-3687

【手数料の表示】

【予納台帳番号】 091329

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子透かし埋め込み装置と方法ならびに電子透かし抽出装置と方法

【特許請求の範囲】

【請求項 1】 ホストデータに第 1 の電子透かしを埋め込む第 1 の埋め込みブロックと、

前記第 1 の電子透かしが埋め込まれたホストデータに前記第 1 の電子透かしの埋め込み位置に関する情報を第 2 の電子透かしとして埋め込む第 2 の埋め込みブロックとを含むことを特徴とする電子透かし埋め込み装置。

【請求項 2】 前記第 1 の埋め込みブロックは、

前記第 1 の電子透かしが埋め込まれるホストデータの埋め込み位置の候補を複数生成する位置情報生成部と、

前記ホストデータの前記埋め込み位置の候補のそれぞれに前記第 1 の電子透かしを埋め込み、複数の第 1 の埋め込みホストデータの候補を生成する第 1 の埋め込み部と、

前記第 1 の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する第 1 の評価部と、

前記耐性の評価値に基づいて前記第 1 の埋め込みホストデータの候補の一つを選択して、前記第 1 の電子透かしが埋め込まれたホストデータとして出力する第 1 の選択部とを含むことを特徴とする請求項 1 に記載の電子透かし埋め込み装置。

【請求項 3】 前記第 2 の埋め込みブロックは、

前記埋め込み位置に関する情報をスクランブルして複数の透かしデータの候補を生成するスクランブル部と、

前記複数の透かしデータの候補をそれぞれ前記第 1 の電子透かしが埋め込まれたホストデータに埋め込み、複数の第 2 の埋め込みホストデータの候補を生成する第 2 の埋め込み部と、

前記第 2 の埋め込みホストデータの候補の各々について、当該電子透かしの耐性を評価する第 2 の評価部と、

前記耐性の評価値に基づいて前記第2の埋め込みホストデータの候補の一つを選択して出力する第2の選択部とを含むことを特徴とする請求項1または2に記載の電子透かし埋め込み装置。

【請求項4】 前記第2の埋め込み部は、前記第2の埋め込みホストデータの候補が、前記第1の電子透かしが埋め込まれた後のホストデータからの許容劣化範囲内で、かつ、前記第1の電子透かしが埋め込まれる前の元のホストデータからの許容劣化範囲内に収まるように制限することを特徴とする請求項3に記載の電子透かし埋め込み装置。

【請求項5】 電子透かしが二重に埋め込まれたホストデータから第1の電子透かしを抽出することにより、第2の電子透かしの埋め込み位置に関する情報を取得する第1の抽出ブロックと、

前記ホストデータから前記第1の電子透かしを除去する除去部と、

前記除去部により前記第1の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第2の電子透かしを抽出する第2の抽出ブロックとを含むことを特徴とする電子透かし抽出装置。

【請求項6】 前記第1の抽出ブロックは、電子透かしが二重に埋め込まれた前記ホストデータからスクランブルされた透かしデータを抽出する抽出部と、

前記スクランブルされた透かしデータのスクランブルを解除して、前記第2の電子透かしの埋め込み位置に関する情報を取得するデスクランブル部とを含むことを特徴とする請求項5に記載の電子透かし抽出装置。

【請求項7】 電子透かしが二重に埋め込まれたホストデータの構造であって、第1の電子透かしの埋め込み位置に関する情報が第2の電子透かしとして可逆埋め込み方式により埋め込まれたことを特徴とするコンピュータにて読み取りおよび利用が可能なデータ構造。

【請求項8】 電子透かしが二重に埋め込まれたホストデータから可逆埋め込み方式で埋め込まれた第1の電子透かしを抽出し、その第1の電子透かしを前記ホストデータから除去した上で、第2の電子透かしを抽出することを特徴とする電子透かし抽出方法。

【請求項9】 前記第1の電子透かしは前記第2の電子透かしの透かし方式

を特定するメタ情報であり、前記第2の電子透かしはこのメタ情報で特定される方式で前記ホストデータから抽出されることを特徴とする請求項8に記載の電子透かし抽出方法。

【請求項10】 電子透かしを二重にホストデータに埋め込む方法であって、第1の電子透かしの埋め込み位置情報を第2の電子透かしとして可逆埋め込み方式により埋め込むことを特徴とする電子透かし埋め込み方法。

【請求項11】 重要度の異なる情報を含む2つの電子透かしをホストデータに埋め込む方法であって、重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込むことを特徴とする電子透かし埋め込み方法。

【請求項12】 前記重要度の高い方の電子透かしを可逆埋め込み方式により前記ホストデータに埋め込むことを特徴とする請求項11に記載の電子透かし埋め込み方法。

【請求項13】 電子透かしが二重に埋め込まれたホストデータから第1の電子透かしを抽出することにより、第2の電子透かしの埋め込み位置に関する情報を取得する工程と、

前記ホストデータから前記第1の電子透かしを除去する工程と、

前記第1の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第2の電子透かしを抽出する工程とをコンピュータに実行させることを特徴とするコンピュータプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、電子透かし技術に関し、特に電子透かしの埋め込み装置と方法、ならびに電子透かしの抽出装置と方法に関する。

【0002】

【従来の技術】

ここ数年、インターネット利用人口が急増し、インターネット利用の新たなステージともいえるブロードバンド時代に入ろうとしている。ブロードバンド通信では通信帯域が格段に広がるため、音声、静止画、動画などデータ量の大きいコ

コンテンツの配信も気軽にできるようになる。このようなデジタルコンテンツの流通が盛んになると、コンテンツの著作権の保護がより一層求められることになる。

【0003】

ネットワーク上に流通するコンテンツのデータは他人に容易にコピーされ、著作権に対する保護が十分ではないのが現状である。そこで著作権を保護するために、コンテンツの作成者や利用者の情報を電子透かしとしてコンテンツデータに埋め込む技術が開発されている。この電子透かし技術を用いることにより、ネットワーク上で流通するコンテンツデータから電子透かしを抽出して、不正利用を検出したり、不正コピーの流通経路を追跡することが可能となる。

【0004】

従来の電子透かしの埋め込み技術には、電子透かしの埋め込んだ後に、その電子透かしの透かし方式を特定するメタ情報をさらに透かしとして埋め込むものがある（たとえば、特許文献1、特許文献2、および特許文献3参照）。

【0005】

また、異なる透かし方式を併用したハイブリッド方式によって電子透かしを二重に埋め込むものもある（たとえば、非特許文献1参照）。

【0006】

【特許文献1】

特開2002-16891号公報（全文、第1-5図）

【特許文献2】

特開2000-287067号公報（全文、第1-7図）

【特許文献3】

特開2001-257865号公報（全文、第1-11図）

【非特許文献1】

大上貴充他、「ハイブリッド式二階層電子透かし方式の提案」、2002年映像情報メディア学会年次大会、8月、2002年

【0007】

【発明が解決しようとする課題】

電子透かしは、不正利用者による改ざんを防止するために、利用者には分からないようにコンテンツデータに埋め込まれる。しかしコンテンツデータは、流通過程や利用過程で、圧縮符号化や各種フィルタリングなどの信号処理が加えられたり、ユーザにより加工されたり、あるいは透かし情報が改ざんされるなど、さまざまな操作を受けることがあり、その過程で埋め込まれた電子透かしデータの一部が変更されたり、消失する可能性がある。したがって電子透かしはこういった操作に対する耐性が要求される。

【0008】

特許文献1～3では、電子透かしを二重に埋め込み、二重化された透かしを順次抽出する方法が提案されているが、2つの透かしは一般に干渉するため、正しく透かしを検出できない場合が生じる。非特許文献1では、ハイブリッド方式によって電子透かしを二重に埋め込むことにより、2つの透かしの干渉性を軽減しているが、下層の透かし方式が限定されるため、汎用性がない。

【0009】

本発明はこうした状況に鑑みてなされたもので、その目的は、耐性の強い電子透かしを埋め込み、電子透かしの検出誤差を低減することの可能な技術の提供にある。

【0010】

【課題を解決するための手段】

本発明のある態様は電子透かし埋め込み装置に関する。この装置は、ホストデータに第1の電子透かしを埋め込む第1の埋め込みブロックと、前記第1の電子透かしが埋め込まれたホストデータに前記第1の電子透かしの埋め込み位置に関する情報を第2の電子透かしとして埋め込む第2の埋め込みブロックとを含む。

【0011】

ホストデータは、電子透かしを埋め込む対象となるオリジナルデータであり、たとえば静止画、動画、音声などのコンテンツデータである。埋め込まれる電子透かしには、オリジナルデータの識別情報、作成者情報、利用者情報などが含まれる。その他、認証を目的として、ホストデータのダイジェストデータ、すなわちホストデータの特徴を端的に表したデータを電子透かしとして埋め込むことも

可能である。

【0012】

本発明の別の態様は電子透かし抽出装置に関する。この装置は、電子透かしが二重に埋め込まれたホストデータから第1の電子透かしを抽出することにより、第2の電子透かしの埋め込み位置に関する情報を取得する第1の抽出ブロックと、前記ホストデータから前記第1の電子透かしを除去する除去部と、前記除去部により前記第1の電子透かしが除去されたホストデータから前記埋め込み位置に関する情報にもとづいて前記第2の電子透かしを抽出する第2の抽出ブロックとを含む。

【0013】

本発明のさらに別の態様は、電子透かしが二重に埋め込まれたホストデータの構造である。このデータ構造は、第1の電子透かしの埋め込み位置に関する情報が第2の電子透かしとして可逆埋め込み方式により埋め込まれた構造を有する。ここで、第1の電子透かしと第2の電子透かしの埋め込まれた順序は任意である。

【0014】

本発明のさらに別の態様は電子透かし抽出方法に関する。この方法は、電子透かしが二重に埋め込まれたホストデータから可逆埋め込み方式で埋め込まれた第1の電子透かしを抽出し、その第1の電子透かしを前記ホストデータから除去した上で、第2の電子透かしを抽出する。この第2の電子透かしは個別の透かし方式で埋め込まれたものであってもよく、第1の電子透かしは第2の電子透かしの透かし方式を特定するためのメタ情報であり、規格化されたものであってもよい。この場合、第2の電子透かしはこのメタ情報で特定される方式でホストデータから抽出されてもよい。可逆埋め込み方式とは、埋め込み処理の逆変換が可能な方式であり、逆変換により埋め込まれた透かしが完全もしくは完全に近い形で除去される特徴をもつ。

【0015】

本発明のさらに別の態様は電子透かし埋め込み方法に関する。この方法は、電子透かしを二重にホストデータに埋め込む方法であって、第1の電子透かしの埋

め込み位置情報を第2の電子透かしとして可逆埋め込み方式により埋め込む。ここで、第1の電子透かしと第2の電子透かしの埋め込み順序は任意である。第1の電子透かしの埋め込み後に第2の電子透かしの埋め込みでもよいが、埋め込み順序を逆にして、第1の電子透かしの埋め込み前に、第1の電子透かしの埋め込み位置情報を第2の電子透かしとして埋め込み、その後に第1の電子透かしの埋め込みでもよい。

【0016】

本発明のさらに別の態様も電子透かし埋め込み方法に関する。この方法は、重要度の異なる情報を含む2つの電子透かしをホストデータに埋め込む方法であって、重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込む。ここでも、重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込む。前記重要度の高い方の電子透かしの耐性を強化して前記ホストデータに埋め込む。電子透かしの耐性とは、電子透かしの埋め込まれたホストデータが改変されるなどの攻撃を受けた場合や、埋め込みホストデータに圧縮符号化やフィルタリングなどの信号処理が施された場合など、埋め込みホストデータに対して何らかの操作が加えられた場合に電子透かしデータがもつ頑強性をいう。

【0017】

なお、以上の構成要素の任意の組み合わせ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【0018】

【発明の実施の形態】

実施の形態1

図1は、実施の形態1に係る電子透かし埋め込み装置100の構成を示す。実透かし埋め込み部112は、入力されたコンテンツVに実透かしXを特定の透かし方式によって埋め込み、実透かし埋め込みコンテンツWを出力する。メタ透かし埋め込み部122は、実透かしXの透かし方式を特定するための実透かし識別情報Y（以下、メタ透かしYともいう）を実透かし埋め込みコンテンツWに透か

しとして埋め込み、実透かしXとメタ透かしYが埋め込まれた二重透かし埋め込みコンテンツUを出力する。メタ透かし埋め込み部122は、メタ透かしYを実透かし埋め込みコンテンツWに埋め込む際、可逆埋め込み方式、すなわち埋め込み処理の逆変換により埋め込まれた透かしを除去して元のデータに復元することができる方式を用いる。

【0019】

コンテンツVの著作権を保護するために、コンテンツのID情報を含む実透かしXは様々な方式で埋め込むことが許されるが、その埋め込み方式を特定する情報を含むメタ透かしYは、規格化された共通の方式で埋め込まれる。

【0020】

図2は、実施の形態1に係る電子透かし抽出装置200の構成を示す。メタ透かし抽出部212は、入力された二重透かし埋め込みコンテンツUからメタ透かしYを抽出し、実透かし選択制御部222およびメタ透かし除去部214に与える。メタ透かし除去部214は、メタ透かし抽出部212により抽出されたメタ透かしYを二重透かし埋め込みコンテンツUから除去し、実透かし埋め込みコンテンツWを取得して切り替え部224に与える。メタ透かしYは可逆埋め込み方式によって埋め込まれているため、メタ透かし除去部214は、埋め込み時の処理の逆変換を行うことによって、二重透かし埋め込みコンテンツUをメタ透かしYを埋め込む前の状態、すなわち実透かし埋め込みコンテンツWに復元することが可能である。

【0021】

実透かし選択制御部222は、メタ透かし抽出部212により抽出されたメタ透かしYにより、実透かしXの透かし方式を特定し、特定された透かし方式の識別情報を切り替え部224に与える。切り替え部224は、特定の透かし方式ごとに用意された複数の特定実透かし抽出部226の内、実透かし選択制御部222により与えられた透かし方式の識別情報にもとづいて、その透かし方式に合ったいずれかの特定実透かし抽出部226を選択し、メタ透かし除去部214から供給される実透かし埋め込みコンテンツWをその選択された特定実透かし抽出部226に供給するように切り替える。

【0022】

特定実透かし抽出部 226 は、特定の透かし方式にもとづいて透かしを抽出する機能を有し、メタ透かし除去部 214 から供給された実透かし埋め込みコンテンツ W からその特定の透かし方式により実透かし X を抽出して出力する。

【0023】

本実施の形態によれば、電子透かし抽出装置 200 において、メタ透かし除去部 214 がメタ透かし Y を除去した上で、実透かし X が抽出されるので、実透かし X とメタ透かし Y の干渉による検出精度の劣化を防ぐことができる。

【0024】

本実施の形態の電子透かし抽出装置 200 は、たとえばコンテンツを提供するサーバなどに設置して、様々な透かし方式により透かしが埋め込まれたコンテンツをユーザに提供するために用いられてもよい。電子透かし抽出装置 200 は、ユーザからコンテンツの要求があったとき、メタ透かしを抽出して、透かし方式を特定して実透かしを抽出し、実透かしに含まれるコンテンツの利用条件などを照合して、ユーザにコンテンツの利用を許諾することができる。

【0025】

実施の形態 2

図 3 は、実施の形態 2 に係る電子透かし埋め込み装置 100 の構成を示す。第 1 透かし埋め込み部 114 は、入力されたコンテンツ V に第 1 透かし X を埋め込み、第 1 透かし埋め込みコンテンツ W を出力し、第 1 透かし X の埋め込み位置情報 Y を第 2 透かし埋め込み部 124 に与える。

【0026】

第 1 透かし埋め込み部 114 は、コンテンツ V の特徴量にもとづいて第 1 透かし X を埋め込む位置を決める。たとえばコンテンツ V が画像データである場合、ピクセル値の分布などを評価して透かしを埋め込んでも目立たない位置を選んだり、エッジ部など画像の高周波成分を埋め込み位置として選んだり、あるいは画像圧縮などの処理に対する耐性を考慮して埋め込み位置を選んだりして、不可視性や耐性を考慮した埋め込み位置を決定する。したがって埋め込み位置はそれぞれのコンテンツ V によって異なる。

【0027】

第2透かし埋め込み部124は、第1透かし埋め込み部114から与えられた埋め込み位置情報Y（以下、第2透かしYともいう）を第1透かし埋め込みコンテンツWに埋め込み、第1透かしXと第2透かしYが埋め込まれた二重透かし埋め込みコンテンツUを出力する。なお、第2透かし埋め込み部124は、可逆埋め込み方式により第2透かしYを第1透かし埋め込みコンテンツWに埋め込む。

【0028】

図4は、実施の形態2に係る電子透かし抽出装置200の構成を示す。第2透かし抽出部216は、入力された二重透かし埋め込みコンテンツUから第2透かし、すなわち埋め込み位置情報Yを抽出し、第1透かし抽出部228および第2透かし除去部218に与える。第2透かし除去部218は、埋め込み処理の逆変換を行って、第2透かしYを二重透かし埋め込みコンテンツUから除去し、第1透かし埋め込みコンテンツWを取得して第1透かし抽出部228に与える。

【0029】

第1透かし抽出部228は、第2透かし抽出部216により抽出された埋め込み位置情報Yをもとに透かしの埋め込み位置を特定し、第1透かし埋め込みコンテンツWから第1透かしXを抽出して出力する。

【0030】

本実施の形態によれば、透かしの埋め込み位置が第2の透かしとしてコンテンツに埋め込まれるため、透かしの埋め込み位置を秘密鍵で提供したり、コンテンツのヘッダに含めて提供するなど、透かしの埋め込み位置を利用者に知らせるための処理が不要になる。

【0031】

実施の形態3

図5は、実施の形態3に係る電子透かし埋め込み装置100の構成を示す。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIで実現でき、ソフトウェア的にはメモリにロードされた電子透かし埋め込み機能のあるプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロッ

クがハードウェアのみ、ソフトウェアのみ、またはそれらの組み合わせによっていろいろな形で実現できることは、当業者には理解されるところである。

【0032】

電子透かし埋め込み装置100は、第1透かし埋め込みブロック110と第2透かし埋め込みブロック120を含む。第1透かし埋め込みブロック110は、ホストデータVに透かし情報Iを埋め込む処理を行い、第1埋め込みホストデータWを出力する。第2透かし埋め込みブロック120は、透かし情報Iの埋め込み位置に関する情報を第1埋め込みホストデータWに第2透かしとして埋め込む処理を行い、第2埋め込みホストデータUを出力する。

【0033】

ここで、ホストデータVは、たとえば音声、静止画、動画などのデータである。透かし情報Iは、そのホストデータVの識別情報、作成者情報、利用者情報など著作権に関する情報、ホストデータVの改ざん検出を行う認証情報、タイムスタンプなどである。

【0034】

第1透かし埋め込みブロック110は、第1透かしデータXをホストデータVの複数の埋め込み位置の候補に埋め込み、透かしの耐性が強くなる候補を選択して、最終的な第1埋め込みホストデータWとして出力する。暗号化部10は、ホストデータVに埋め込むべき透かし情報Iを秘密鍵Kにより暗号化し、第1透かしデータXを出力する。透かし情報の暗号化を行わない場合には、暗号化部10の構成は省略してもよい。

【0035】

位置検出部12は、ホストデータVの特徴と秘密鍵Kにもとづいて第1透かしデータXの埋め込み位置Pを決定し、第1透かし埋め込み部14は、秘密鍵Kを用いて、ホストデータVの埋め込み位置Pに第1透かしデータXを埋め込み、第1埋め込みホストデータWを出力する。図5では、暗号化部10、位置検出部12、第1透かし埋め込み部14、第2透かし埋め込みブロック120の変更部16および第2透かし埋め込み部18に秘密鍵Kの情報が入力されているが、各部に入力される秘密鍵Kの情報はお互いに独立であってもよい。また、秘密鍵Kの

情報の一部が従属する内容であってもよく、完全に同一のものであってもよい。さらには、秘密鍵Kに依存しない埋め込み方式を採用してもよい。位置検出部12と埋め込み部14は協同して、複数の埋め込み位置Pを生成し、それぞれの埋め込み位置Pに第1透かしデータXを埋め込み、複数の埋め込みホストデータWの候補を生成し、それらの候補の一つを選択する機能をもつ。

【0036】

第2透かし埋め込みブロック120は、第1透かしデータXの埋め込み位置Pの識別情報を含む第2透かしデータYをスクランブルして、第1埋め込みホストデータWに埋め込み、第2埋め込みホストデータUを出力する。変更部16は、第2透かしデータY、第1埋め込みホストデータW、および秘密鍵Kを用いて、第2透かしデータYをスクランブルし、スクランブルされた第2透かしデータY'を出力する。

【0037】

第2透かし埋め込み部18は、秘密鍵Kを用いて、スクランブルされた透かしデータY'を第1埋め込みホストデータWに埋め込み、第2埋め込みホストデータUを出力する。秘密鍵Kに依存しない埋め込み方式を用いてもよい。

【0038】

変更部16と第2透かし埋め込み部18は協同して、複数のスクランブルされた透かしデータY'を生成し、それぞれを第2埋め込みホストデータWに埋め込み、複数の第2埋め込みホストデータUの候補を生成し、それらの候補の一つを選択する機能をもつ。

【0039】

図6は第1透かし埋め込みブロック110の位置検出部12および第1透かし埋め込み部14の機能構成図である。ECC (Error Correction Code) 部24は第1透かしデータXに誤り訂正のためのパリティを付加した透かしデータX_cを生成する。ECC部24は、透かしビットの検出率を向上させるためのオプションであって、アプリケーションによっては必要ない場合もあり、この構成を省略してもよい。

【0040】

位置情報生成部 60 は、ホストデータ V について L_1 個の埋め込み位置 P の候補をランダムに生成する。第 1 埋め込み部 26 は L_1 個の埋め込み位置 P の候補のそれぞれに透かしデータ X_c を埋め込み、 L_1 種類の第 1 埋め込みホストデータ W の候補を生成する。

【0041】

L_1 個の SNR 計算部 28 は、 L_1 種類の第 1 埋め込みホストデータ W の候補のそれぞれについて、第 1 透かしデータ X の耐性を評価する。セクタ 32 は、耐性の評価値が最良である第 1 埋め込みホストデータ W の候補を選択し、それを最終的な第 1 埋め込みホストデータ W として出力し、その場合の第 1 透かしデータ X の埋め込み位置情報 P^* を出力する。

【0042】

埋め込み位置の候補は、一例としてテーブルマッチングによりランダムに生成される。位置情報生成部 60 は、埋め込み位置の候補を識別するための識別情報と埋め込む位置とを対応づけたテーブルを備え、このテーブルを参照して、埋め込み位置の候補の識別データに対応づけて埋め込み位置の候補を生成する。このテーブルは、透かしデータの第 1 ビットについて、たとえば、「識別番号 0 の場合は (1, 29) の位置、識別番号 1 の場合は (983, 251) の位置、・・・、識別番号 15 の場合は (542, 37) の位置に埋め込む」といった識別番号と埋め込み座標との対応関係を格納する。第 2 番目から第 n_1 番目のビットについてもそれぞれ埋め込み位置が異なる対応関係が格納される。埋め込み位置は何らかの方法でランダムに生成されたものである。

【0043】

図 7 は第 2 透かし埋め込みブロック 120 の変更部 16 および第 2 透かし埋め込み部 18 の機能構成図である。第 2 透かし埋め込みブロック 120 は第 1 透かし埋め込みブロック 110 から第 1 埋め込みホストデータ W と埋め込み位置情報 P^* を供給される。埋め込み位置情報 P^* は、第 1 透かしデータ X の各ビットの埋め込み位置の識別情報であり、この識別情報を含む透かしビットの系列を第 2 透かしデータ Y と表記する。 L_2 個のマルチプレクサ 20 は、第 2 透かしデータ Y の先頭にそれぞれ初期データ $C_0 \sim C_{L_2-1}$ を挿入した L_2 種類のビット系

列 Y_b を生成する。 L_2 個のスクランブラ 22 は L_2 種類のビット系列をそれぞれスクランブルして、 L_2 種類のスクランブルされた透かしデータ Y'_b を生成する。 L_2 個の ECC 部 24 は L_2 種類のスクランブルされた透かしデータ Y'_b のそれぞれに誤り訂正のためのパリティを付加した透かしデータ Y'_c を生成する。

【0044】

L_2 個の第2埋め込み部 27 は、可逆埋め込み方式により、 L_2 種類のスクランブルされた透かしデータ Y'_c のそれぞれを第1埋め込みホストデータ W に埋め込み、 L_2 種類の第2埋め込みホストデータ U の候補を生成する。 L_2 個の SNR 計算部 28 は、 L_2 種類の第2埋め込みホストデータ U の候補のそれぞれについて、透かしデータ Y の耐性を評価する。セクタ 30 は、耐性の評価値が最良である第2埋め込みホストデータ U の候補を選択し、それを最終的な第2埋め込みホストデータ U として出力する。

【0045】

図8は、実施の形態3に係る電子透かし抽出装置 200 の構成を示す。電子透かし埋め込み装置 100 により電子透かしが埋め込まれた第2埋め込みホストデータ U は、ネットワーク上で流通し、コンピュータにおいて利用される。その過程で第2埋め込みホストデータ U は圧縮符号化や改ざんなどの操作を受ける。画像データであれば、JPEG 圧縮、フィルタリング、量子化、色補正などの信号処理や、スケーリング、クロッピング、回転、並行移動等の幾何学的な変換など有用性のある操作が施されたり、電子透かしを除去したり改変するなどの不正な攻撃が加えられたりする。そのような操作による変形を第2埋め込みホストデータ U に対するノイズ N とみなし、ノイズ N が付加した第2埋め込みホストデータ U を第2埋め込みホスト信号 \hat{U} ($=U+N$) とする。電子透かし抽出装置 200 は、第2埋め込みホスト信号 \hat{U} から埋め込まれた透かしデータ X を抽出する処理を行う。

【0046】

電子透かし抽出装置 200 は、第2透かし抽出ブロック 210 と第1透かし抽出ブロック 220 を含む。第2透かし抽出ブロック 210 は、第2埋め込みホス

ト信号 U^{\wedge} から第2透かしデータ Y を抽出する処理を行う。第2抽出部 40 は、秘密鍵 K を用いて、第2埋め込みホスト信号 U^{\wedge} に埋め込まれた第2透かしデータ Y^{\wedge}_c を抽出する。ECC復号部 44 はこの第2透かしデータ Y^{\wedge}_c に付加されているパリティビットを用いて誤り訂正を行い、第2透かしデータ Y^{\wedge}_b を生成する。デスクランブラ 46 は秘密鍵 K を用いて、誤り訂正後の第2透かしデータ Y^{\wedge}_b のスクランブルを解除し、先頭部の初期データを取り除いて第2透かしデータ Y^{\wedge} を出力する。この第2透かしデータ Y^{\wedge} には第1透かしデータ X の埋め込み位置情報 P^{\wedge} が含まれ、この埋め込み位置情報 P^{\wedge} は電子透かし抽出装置 200 の第1抽出部 48 に供給される。

【0047】

第2透かし抽出ブロック 210 の第2透かし除去部 42 は、図7の第2透かし埋め込みブロック 120 の第2埋め込み部 27 の埋め込み処理の逆変換を行うことにより、第2抽出部 40 により抽出された第2透かしデータ Y^{\wedge}_c を第2埋め込みホスト信号 U^{\wedge} から除去し、第1埋め込みホスト信号 W^{\wedge} を出力する。

【0048】

第1透かし抽出ブロック 220 は、第2透かし抽出ブロック 210 の第2透かし除去部 42 から供給される第1埋め込みホスト信号 W^{\wedge} から第1透かしデータ X を抽出する処理を行う。第1抽出部 48 は、第2透かし抽出ブロック 210 のデスクランブラ 46 が出力する第2透かしデータ Y^{\wedge} から埋め込み位置情報 P^{\wedge} を取得し、秘密鍵 K を用いて、第2透かし抽出ブロック 210 の第2透かし除去部 42 から得た第1埋め込みホスト信号 W^{\wedge} から埋め込み位置情報 P^{\wedge} で示される位置に埋め込まれた第1透かしデータ X^{\wedge}_c を抽出する。ECC復号部 45 は、この第1透かしデータ X^{\wedge}_c に付加されているパリティビットを用いて誤り訂正を行い、第1透かしデータ X^{\wedge}_b を生成して出力する。

【0049】

第1抽出部 48 は、一例として前述のテーブルマッチングの方法を用い、図6の位置情報生成部 60 が参照するテーブルと同じテーブルを参照して、埋め込み位置情報 P^{\wedge} にもとづき、埋め込み位置の識別情報情報に対応づけられた埋め込み位置を特定し、第1透かしデータ X^{\wedge} をその位置から抽出する。

【0050】

なお、上記の説明では、図7で示したように、 L_2 種類の透かしデータの候補を生成するために、 L_2 個のマルチプレクサ20、スクランブラ22、ECC部24、第2埋め込み部27、およびSNR計算部28が並列に設けられたが、これらの部材を単一構成にして、 L_2 種類の透かしデータの候補を逐次的に生成、評価して最適な候補を選択してもよい。透かしデータの候補を逐次生成し、埋め込み強度が所望の基準値以上である候補が得られた時点で、その候補を最終的な埋め込みホストデータWとして選択し、そのような候補が生成されなければ、 L_2 個の埋め込みホストデータの候補の中から埋め込み強度が最大であるものを最終的な埋め込みホストデータWとして選択することができる。

【0051】

以上の構成の電子透かし埋め込み装置100および電子透かし抽出装置200による電子透かしの埋め込みと抽出の手順を説明する。

【0052】

(1) 第1透かしデータXの埋め込み手順

図9は、電子透かし埋め込み装置100の第1透かし埋め込みブロック110による第1透かしデータXの埋め込み手順を説明するフローチャートである。位置情報生成部60は、第1透かしデータXの L_1 個の埋め込み位置候補 P^k ($k=0, \dots, L_1-1$)を生成する(S30)。

【0053】

ECC部24は、第1透かしデータXに誤り訂正のためのパリティを付加し、第1埋め込み部26は、ホストデータVの L_1 個の埋め込み位置の候補 P^k のそれぞれに第1透かしデータXを埋め込む(S32)。

【0054】

第1透かしデータXは次のように n_1 ビットのビット系列で表される。

$$X = \{x_0, x_1, \dots, x_{n_1-1}\}$$

この n_1 ビットの第1透かしデータXの埋め込み位置の候補 P^k に対応するホストデータVのサンプルの集合のペア($V+k, V-k$)を次のように定義する。サンプルの集合 $V+k, V-k$ はそれぞれ n_1 個の要素をもつ。なお、ホストデ

ータ V は、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえば DCT 変換、FFT 変換、DWT 変換などの処理後のサンプルなどにより表現される。

【0055】

$$V+k = \{v+k_0, v+k_1, \dots, v+k_{n_1-1}\}$$

$$V-k = \{v-k_0, v-k_1, \dots, v-k_{n_1-1}\}$$

ここでサンプルの集合 $V+k$ 、 $V-k$ の要素である各サブセット $v+k_i$ 、 $v-k_i$ は、次のようにホストデータ V の m_1 個のサンプルデータからなる。

$$v+k_i = \{v+k_i, 0, v+k_i, 1, \dots, v+k_i, m_1-1\}$$

$$v-k_i = \{v-k_i, 0, v-k_i, 1, \dots, v-k_i, m_1-1\}$$

【0056】

第 1 透かしデータ X の各ビットを埋め込み位置の候補 P^k に対応した L_1 個のサンプルの集合のペア $(V+k, V-k)$ に次のように埋め込み、 L_1 種類の第 1 埋め込みホストデータの候補 W^k を生成する。

【0057】

$$w+k_{i,j} = v+k_{i,j} + \alpha^+_{i,j} \cdot x_i$$

$$w-k_{i,j} = v-k_{i,j} - \alpha^-_{i,j} \cdot x_i$$

ここで $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケーリングパラメータであり、いずれも正の値である。あるいは、 $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵 K によって生成される正の値であってもよい。この場合、透かしの埋め込み強度は減少するが、埋め込まれた透かしの秘匿性は向上する。

【0058】

このようにして、第 1 透かしデータの各ビット x_i は各サブセット $v+k_i$ 、 $v-k_i$ のそれぞれ m_1 個のサンプルに重複して埋め込まれる。重複の数 m_1 が大きいほど、透かしビットが失われる可能性が低くなり、検出誤差が小さくなる一方で、ホストデータに埋め込むことができる透かしのビット数が減少する。 $\alpha^+_{i,j}$ および $\alpha^-_{i,j}$ は、視覚上の劣化を検知できないようにピクセル毎に

設定される値であり、原理的には、埋め込むピクセル数 m_1 を増やしても、人間の視覚上、画質の劣化は検知されない。しかし、1ビットを埋め込むのに費やすピクセル数が増加するということは、埋め込み領域には制限があるため、埋め込むことができるビット数が減少することを意味し、したがって埋め込み率の低下を招くことになる。

【0059】

SNR計算部28は、 L_1 種類の第1埋め込みホストデータの候補 W^k に対して第1透かしデータXの耐性、すなわち埋め込み強度を評価し(S34)、セレクタ32は埋め込み強度が最大となる第1埋め込みホストデータの候補 W^k を最終的な第1埋め込みホストデータWとして選択する(S36)。

【0060】

埋め込み強度の評価は、ホストデータVを第1透かしデータXに対するノイズとみなして、埋め込まれた透かしデータXに対して検出される透かしデータの分散を計算することにより行われる。分散が小さいほど、耐性が強いと考えることができる。第1埋め込みホストデータの候補のペア($W+k$, $W-k$)に対して次式によりSN比を評価して、最適な候補Kを選択する。

【0061】

$$K = \arg \max_k (P_k / \sigma_k^2)$$

$$P_k = \sum_{i=0}^{n_1-1} \left| \sum_{j=0}^{m_1-1} (w+k_{i,j} - w-k_{i,j}) \right|^2 / n$$

$$\sigma_k^2 = \sum_{i=0}^{n_1-1} \left| \sum_{j=0}^{m_1-1} (w+k_{i,j} - w-k_{i,j}) - P_k \right|^2 / n$$

【0062】

(2) 第2透かしデータYの埋め込み手順

図14は、電子透かし埋め込み装置100の第2透かし埋め込みブロック120による第2透かしデータYの埋め込み手順を説明するフローチャートである。フローチャートの説明にあたり、図10から図13を適宜参照する。

【0063】

第2透かし埋め込みブロック120は第1透かし埋め込みブロック110から

第1透かしデータXの埋め込み位置情報P*を得る。マルチプレクサ20は、この埋め込み位置情報P*を識別情報として含む第2透かしデータYの先頭にL₂種類の初期データを挿入してL₂個の符号系列を生成し(S10)、スクランブラ22は、それらの符号系列をスクランブルしてL₂種類のスクランブルされた第2透かしデータY'を生成する(S12)。

【0064】

図10は、第2透かしデータYとL₂種類のスクランブルされた第2透かしデータY'との関係を示す。n₂ビットの第2透かしデータYの先頭に、r₂ビットの冗長語を識別データID[0]～ID[L₂-1]として付加し、L₂種類の第2透かしデータの候補を作成する。最大2^{r₂}種類の候補が作成される。これらの候補に含まれる第2透かしデータYのビット列はこれから述べるスクランブル方式により、スクランブルされる。

【0065】

スクランブル方式の一例として、伝送や磁気記録におけるデジタル変調の際に利用されるGS (Guided Scramble) 方式を採用する。GS方式は、ある一定のデータブロック長からなる情報系列に対して、L種類の符号系列を生成し、これらを次に送信する符号系列の候補として扱う。これらの候補の中から、伝送媒体の性質に合わせて最適なものを選択して最終的な符号系列とする。このGS方式により、多様性に富んだ符号系列の候補を簡単な方法で生成することができる。

【0066】

第2透かし埋め込みブロック120におけるマルチプレクサ20とスクランブラ22がGS符号化器の一部として機能する。GS符号化器は、nビットからなる情報系列D(x)の直前にL種類のrビットの冗長語c_i (i=0, ..., L-1)を付加し、L種類の符号系列c_ixⁿ+D(x)を生成する。この符号系列の符号長は(n+r)ビットとなる。このようにして冗長語が付加された符号系列に対して、次式のようにN次元のスクランブル多項式S(x)で除算することにより商T_i(x)を求める。

【0067】

$$T_i(x) = Q S(x) [(c_i x^n + D(x)) x^N] \quad (1)$$

ただし、 $Q_a[b]$ は b を a で除算した商を示す。商集合 $\{T_0(x), \dots, T_{L-1}(x)\}$ がスクランブル後の符号系列の候補である。これらの候補の各々について、その符号系列が実際に用いられた際の性能を評価し、その評価値が最良であるものを最終的な符号系列として選択する。

【0068】

透かし抽出時には、第2透かし抽出ブロック210におけるデスクランブラ46がGS復号器として機能し、符号系列に $S(x)$ を乗算し、下位 N ビットと上位 r ビットの変換情報を捨てることにより、元の情報系列 $D(x)$ が得られる。

【0069】

ここでスクランブル多項式 $S(x)$ として、 $S(x) = x^r + 1$ を用いた場合を説明する。 $n \bmod r = 0$ の場合、(1) 式は次式に示す畳み込み演算で表現可能である。

【0070】

$$t_j = d_j (+) c_i \quad (j=0)$$

$$t_j = d_j (+) t_{j-1} \quad (j=1, \dots, n/r-1)$$

ただし、 $i=0, \dots, L-1$ であり、 d_j は元の情報系列 $D(x)$ を r ビットずつ区切ったビット列、 t_j は変換後の符号系列 $T_i(x)$ の先頭の r ビットの冗長語 c_i 以降を r ビットずつ区切ったビット列である。また $(+)$ は排他的論理和 (EX-OR) 演算を示す。

【0071】

図11はこの透かし埋め込み時の畳み込み演算を説明する図である。たとえば、 $n=6$ 、 $r=2$ の場合を考える。元の情報系列 $D(x) = (1, 0, 1, 0, 0, 1)$ に対して、冗長語 $c_0 = (0, 0)$ を付加して、変換後の符号系列 $T_0(x)$ を生成する。上記の符号化時の畳み込み演算により、 $t_0 = d_0 (+) c_0 = (1, 0) (+) (0, 0) = (1, 0)$ 、 $t_1 = d_1 (+) t_0 = (1, 0) (+) (1, 0) = (0, 0)$ 、 $t_2 = d_2 (+) t_1 = (0, 1) (+) (0, 0) = (0, 1)$ となり、変換後の符号系列 $T_0 = (0, 0, 1, 0, 0, 0, 0, 1)$ が得られる。ここで変換後の符号系列 T_0 の先頭の2ビットは冗長語 c_0 であることに注意する。

【0072】

同様に、冗長語 $c_1 = (0, 1)$ 、 $c_2 = (1, 0)$ 、 $c_3 = (1, 1)$ に対して、それぞれ変換後の符号系列 $T_1 = (0, 1, 1, 1, 0, 1, 0, 0)$ 、 $T_2 = (1, 0, 0, 0, 1, 0, 1, 1)$ 、 $T_3 = (1, 1, 0, 1, 1, 1, 1, 0)$ が得られる。

【0073】

透かし抽出時は次式のように畳み込み演算を行うことにより、元の情報系列 $D(x)$ が得られる。

【0074】

$$d_j = t_j (+) c_i \quad (j=0)$$

$$d_j = t_j (+) t_{j-1} \quad (j=1, \dots, n/r-1)$$

【0075】

図12はこの透かし抽出時の畳み込み演算を説明する図である。前述の例において、変換後の符号化系列 $T_0 = (0, 0, 1, 0, 0, 0, 0, 1)$ が与えられると、先頭の2ビットから冗長語 $c_0 = (0, 0)$ が得られ、上記の復号時の畳み込み演算により、 $d_0 = t_0 (+) c_0 = (1, 0) (+) (0, 0) = (1, 0)$ 、 $d_1 = t_1 (+) t_0 = (0, 0) (+) (1, 0) = (1, 0)$ 、 $d_2 = t_2 (+) t_1 = (0, 1) (+) (0, 0) = (0, 1)$ となり、元の情報系列 $D(x) = (1, 0, 1, 0, 0, 1)$ が得られる。他の変換後の符号化系列 T_1 、 T_2 、 T_3 についてもこの畳み込み演算により、元の情報系列 $D(x)$ が得られる。

【0076】

再び図14を参照する。スクランブラ22によって生成された L_2 種類のスクランブルされた透かしデータ Y' は、ECC部24により誤り訂正のためのパリティを付加された後に、第2埋め込み部27により第1埋め込みホストデータ W に埋め込まれる (S14)。

【0077】

図13(a)、(b)は、スクランブルされた透かしデータ Y' の埋め込み方法を説明する図である。 L_2 種類のスクランブルされた透かしデータ Y' を y^0

, y^1_1, \dots, y^{L2-1} とする。各透かしデータの候補のビット系列は、次式のように表される。先頭の r_2 ビットは識別データである。また、スクランブル処理後のビット 0 は、 -1 に置き換えて、以下の処理を行う。

【0078】

$$y^0 = \{-1, \dots, -1, -1, y^0_0, y^0_1, \dots, y^0_{n2-1}\}$$

$$y^1 = \{-1, \dots, -1, 1, y^1_0, y^1_1, \dots, y^1_{n2-1}\}$$

...

$$y^{L2-1} = \{1, \dots, 1, 1, y^{L2-1}_0, y^{L2-1}_1, \dots, y^{L2-1}_{n2-1}\}$$

【0079】

($n_2 + r_2$) ビットの透かしデータ Y の埋め込み対象として選択された第 1 埋め込みホストデータ W から、第 2 透かし埋め込み用の秘密鍵を用いて、サンプル集合のペア (Ω^+ , Ω^-) を次のように選択する。このサンプル集合 (Ω^+ , Ω^-) は第 1 埋め込みホストデータ W から第 2 透かし埋め込み用の秘密鍵にもとづいて選択される集合であり、第 1 透かしデータ X の埋め込み対象として第 1 透かし埋め込み用の秘密鍵にもとづいて選択されたサンプル集合 (V^+ , V^-) とは独立に選択される。したがって、第 1 透かし埋め込み後のサンプル集合 (W^+ , W^-) とは区別する意味で、ここでは第 2 透かしの埋め込み対象のサンプル集合を (Ω^+ , Ω^-) と表記している。サンプルの集合 Ω^+ , Ω^- は次のようにそれぞれ ($n_2 + r_2$) 個の要素をもつ。なお、第 1 埋め込みホストデータ W は、空間軸上のサンプル、時間軸上のサンプル、周波数軸上のサンプル、たとえば DCT 変換、FFT 変換、DWT 変換などの処理後のサンプルなどにより表現される。

【0080】

$$\Omega^+ = \{\omega^+_0, \omega^+_1, \dots, \omega^+_{n2+r2-1}\}$$

$$\Omega^- = \{\omega^-_0, \omega^-_1, \dots, \omega^-_{n2+r2-1}\}$$

ここでサンプルの集合 Ω^+ , Ω^- の要素である各サブセット ω^+_i , ω^-_i は、次のように第 1 埋め込みホストデータ W の m_2 個のサンプルデータからなる。

【0081】

$$\omega^+ i = \{\omega^+ i, 0, \omega^+ i, 1, \dots, \omega^+ i, m_2 - 1\}$$

$$\omega^- i = \{\omega^- i, 0, \omega^- i, 1, \dots, \omega^- i, m_2 - 1\}$$

【0082】

第2透かしデータの候補 y^k ($k=0, \dots, L_2-1$) をサンプルの集合のペア (Ω^+, Ω^-) に次のように埋め込み、 L_2 種類の第2埋め込みホストデータの候補 U^k を生成する。

【0083】

$$u^+ k i, j = \omega^+ i, j + \beta^+ i, j \cdot y^k i$$

$$u^- k i, j = \omega^- i, j - \beta^- i, j \cdot y^k i$$

ここで $\beta^+ i, j$ および $\beta^- i, j$ は人間の視覚モデルにもとづいて知覚されるノイズを減少するためのスケーリングパラメータであり、いずれも正の値である。あるいは、 $\beta^+ i, j$ および $\beta^- i, j$ は、ある確率分布、たとえばガウシアン分布、一様分布などに従うように、秘密鍵 K によって生成される正の値であってもよい。このようにして、 k 番目の第2透かしデータの候補の各ビット $y^k i$ は各サブセット $\omega^+ i, \omega^- i$ のそれぞれ m_2 個のサンプルに重複して埋め込まれる。

【0084】

各サブセット $\omega^+ i, \omega^- i$ は、一例として、特定の DCT (Discrete Cosine Transform) ブロックを示しており、透かしビットの埋め込み対象として選ばれる m_2 個のサンプルデータは、その DCT ブロックに含まれる m_2 個の DCT 係数である。図 13 (a)、(b) は、 8×8 の DCT ブロックのペア $\omega^+ i, \omega^- i$ のそれぞれ m_2 個の DCT 係数に第2透かしデータ $y^k i$ が埋め込まれる様子を示している。ブロックペア $\omega^+ i, \omega^- i$ および m_2 個の DCT 係数は、秘密鍵 K に基づいて選択される。

【0085】

図 14 に戻り、SNR 計算部 28 は、 L_2 種類の第2埋め込みホストデータの候補 U^k に対して第2透かしデータ y^k の耐性、すなわち埋め込み強度を評価し (S16)、セクタ 30 は埋め込み強度が最大となる第2埋め込みホストデー

タの候補 U^k を最終的な第2埋め込みホストデータ U として選択する (S18)

。

【0086】

埋め込み強度の評価式を与える前に、第2埋め込みホストデータ U に対して信号処理や画像処理などにより変形が加えられた場合に、第2透かしデータ Y^{\wedge} がどのように検出されるかを検討する。第2埋め込みホストデータ U に加えられる変形をノイズ N として扱い、ノイズ N が加わった埋め込みホストデータ U を第2埋め込みホスト信号 U^{\wedge} と呼ぶ。この第2埋め込みホスト信号 U^{\wedge} から第2透かしデータ Y^{\wedge} を抽出する方法を説明する。第2埋め込みホスト信号の集合のペア $(U^{\wedge+}, U^{\wedge-})$ を次のように定義する。第2埋め込みホスト信号の集合 $U^{\wedge+}$, $U^{\wedge-}$ は次のようにそれぞれ $(n_2 + r_2)$ 個の要素をもつ。

【0087】

$$U^{\wedge+} = \{u^{\wedge+}_0, u^{\wedge+}_1, \dots, u^{\wedge+}_{n_2 + r_2 - 1}\}$$

$$U^{\wedge-} = \{u^{\wedge-}_0, u^{\wedge-}_1, \dots, u^{\wedge-}_{n_2 + r_2 - 1}\}$$

ここで第2埋め込みホスト信号の集合 $U^{\wedge+}$, $U^{\wedge-}$ の要素である各サブセット $u^{\wedge+}_i$, $u^{\wedge-}_i$ は、電子透かしの埋め込み位置に対応して、次のように埋め込みホスト信号 U^{\wedge} の m_2 個のサンプルデータからなる。

$$u^{\wedge+}_i = \{u^{\wedge+}_{i,0}, u^{\wedge+}_{i,1}, \dots, u^{\wedge+}_{i,m_2 - 1}\}$$

$$u^{\wedge-}_i = \{u^{\wedge-}_{i,0}, u^{\wedge-}_{i,1}, \dots, u^{\wedge-}_{i,m_2 - 1}\}$$

【0088】

第2透かしビット y^k_i を検出するために、次の検出値 z_i を計算する。

$$\begin{aligned} z_i &= \sum_{j=0}^{m_2 - 1} (u^{\wedge+}_{i,j} - u^{\wedge-}_{i,j}) \\ &= \sum_{j=0}^{m_2 - 1} [(u^+_{i,j} + n^+_{i,j}) - (u^-_{i,j} + n^-_{i,j})] \\ &= \sum_{j=0}^{m_2 - 1} [(\omega^+_{i,j} - \omega^-_{i,j}) + (\beta^+_{i,j} - \beta^-_{i,j}) \cdot y^k_i + (n^+_{i,j} - n^-_{i,j})] \end{aligned}$$

ここで $\sum_{j=0}^{m_2 - 1} (\omega^+_{i,j} - \omega^-_{i,j})$ は m_2 が十分に大きいとき、一般にガウス分布に従い、0 に近づく。またノイズの項 $\sum_{j=0}^{m_2 - 1} (n^+_{i,j} - n^-_{i,j})$ についても同様に0 に近づく。したがって、 z_i は \sum_j

$= 0^{m_2-1} [(\beta^{+i, j} + \beta^{-i, j}) \cdot y^{k_i}]$ の値で近似できる。 $(\beta^{+i, j} + \beta^{-i, j})$ は正であるから、第2透かしビット y^{k_i} が1ならば z_i は正であり、第2透かしビット y^{k_i} が-1ならば z_i は負である。したがって z_i の正負により第2透かしビット y^{k_i} の値を判定することができる。

【0089】

埋め込み強度の評価は、第1埋め込みホストデータ W を第2透かしデータ Y に対するノイズとみなして、埋め込まれた透かしデータ Y に対して検出される透かしデータの分散を計算することにより行われる。分散が小さいほど、耐性が強いと考えることができる。第2埋め込みホストデータの候補のペア $(U+k, U-k)$ に対して次式により SN 比を評価して、最適な候補 K を選択する。

【0090】

$$K = \arg \max_k (P_k / \sigma_k^2)$$

$$P_k = \sum_{i=0}^{n_2+r_2-1} | \sum_{j=0}^{m_2-1} (u+k_{i,j} - u-k_{i,j}) |^2 / (n_2+r_2)$$

$$\sigma_k^2 = \sum_{i=0}^{n_2+r_2-1} | \sum_{j=0}^{m_2-1} (u+k_{i,j} - u-k_{i,j}) - P_k^{1/2} \cdot y^{k_i} |^2 / (n_2+r_2)$$

【0091】

第2透かしビット y^{k_i} が $\{1, -1\}$ のいずれであるかを判定するための前述の検出値 z_i は、第2埋め込みホストデータ U にノイズが付加される前の状態では、 $z_i = \sum_{j=0}^{m_2-1} (u+k_{i,j} - u-k_{i,j})$ で与えられることを考慮すると、分散 σ_k^2 は、第2透かしビットに関する検出値 z_i と実際に埋め込まれた第2透かしビットの平均値 $P_k^{1/2} \cdot y^{k_i}$ との差の自乗を $i = 0, \dots, n_2+r_2-1$ について評価して平均化したものであると言える。ただし、 P_k は検出値 z_i の $i = 0, \dots, n_2+r_2-1$ についての自乗平均であり、埋め込まれた透かしの平均パワーを示す。したがって、埋め込まれた第2透かしデータ y^k と抽出される透かしデータとの間のユークリッド距離が小さく、第2透かしビットを抽出するための検出値の絶対値が大きいほど、 P_k / σ_k^2 の値は大きくなる。言い換えれば、 P_k / σ_k^2 が最大となる候補を選択することは、第2透かしビットの検出誤差が最小である候補を選択することを意

味する。

【0092】

検出値 z_i について、 $\omega^+_{i,j} > \omega^-_{i,j}$ かつ $y^k_i = 1$ ならば $z_i \gg 0$ となり、 $\omega^+_{i,j} < \omega^-_{i,j}$ かつ $y^k_i = -1$ ならば $z_i \ll 0$ となる。したがって前述の評価により最適な第2透かしデータ y^k の候補を選択することは、検出値 z_i による第2透かしビット y^k_i の検出性能を向上させるために、 $\omega^+_{i,j} > \omega^-_{i,j}$ ならば $y'_i = 1$ となり、 $\omega^+_{i,j} < \omega^-_{i,j}$ ならば $y'_i = -1$ となるように、元の透かしビット y_i を y'_i に変更することを意味する。これがGS方式のガイディングルールであり、これにより検出値 z_i のレスポンスが改善する。

【0093】

(3) 第2透かしYの抽出手順

第2透かし抽出ブロック210の第2抽出部40は、ノイズの付加された第2埋め込みホスト信号 \hat{U} を受け取ると、ECC復号部44が硬入力 of 復号器で構成される場合には、検出値 z_i を次式に示すように計算し、検出値 z_i の正負で、第2透かしビット \hat{y}_i が $\{-1, 1\}$ のいずれであるかを判定し、第2透かしデータ \hat{Y} を得る。また、ECC復号部44が軟入力 of 復号器で構成される場合には、検出値 z_i を $\{-1, 1\}$ に硬判定することなく、そのまま、ECC復号部44に送る。

【0094】

$$\begin{aligned} z_i &= \sum_{j=0}^{m2-1} (\hat{u}^+_{i,j} - \hat{u}^-_{i,j}) \\ &= \sum_{j=0}^{m2-1} [(\hat{u}^+_{i,j} + n^+_{i,j}) - (\hat{u}^-_{i,j} + n^-_{i,j})] \\ &\doteq \sum_{j=0}^{m2-1} [(\omega^+_{i,j} - \omega^-_{i,j}) + (\beta^+_{i,j} + \beta^-_{i,j}) \cdot y_i] \end{aligned}$$

【0095】

抽出された第2透かしデータ \hat{Y} はさらにECC復号部44により誤り訂正がなされ、デスクランブラ46によりスクランブルを解除されて出力される。

【0096】

(4) 第2透かしの除去手順

第2透かし抽出ブロック210の第2透かし除去部42による第2透かしの除去手順を説明する。第2埋め込みホスト信号 U^{\wedge} から検出された第2透かしデータ Y^{\wedge} による変化分を次のように除去して第1埋め込みホスト信号 W^{\wedge} を取得する。

$$\begin{aligned}\omega^{\wedge+}_{i,j} &= u^{\wedge+}_{i,j} - \beta^{\wedge+}_{i,j} \cdot y^{\wedge}_{i,j} \\ &= \omega^+_{i,j} + (\beta^+_{i,j} \cdot y_{i,j} - \beta^{\wedge+}_{i,j} \cdot y^{\wedge}_{i,j}) + n^+_{i,j} \\ &= \omega^+_{i,j} + q^+_{i,j} + n^+_{i,j} \\ \omega^{\wedge-}_{i,j} &= u^{\wedge-}_{i,j} + \beta^{\wedge-}_{i,j} \cdot y^{\wedge}_{i,j} \\ &= \omega^-_{i,j} - (\beta^-_{i,j} \cdot y_{i,j} - \beta^{\wedge-}_{i,j} \cdot y^{\wedge}_{i,j}) + n^-_{i,j} \\ &= \omega^-_{i,j} - q^-_{i,j} + n^-_{i,j}\end{aligned}$$

ここで、 $\beta^{\wedge+}_{i,j}$ および $\beta^{\wedge-}_{i,j}$ は上述の人間の視覚モデルによるスケーリングパラメータ $\beta^+_{i,j}$ および $\beta^-_{i,j}$ の近似値である。第2透かしに関するスケーリングパラメータが、視覚モデルではなく、秘密鍵に基づいて計算されるデータの場合には、第2透かしの埋め込み時、抽出時共に同一の値を発生させることができるため、 $\beta^+_{i,j} = \beta^{\wedge+}_{i,j}$ 、 $\beta^-_{i,j} = \beta^{\wedge-}_{i,j}$ となり、さらに、第2透かしビット $y^{\wedge}_{i,j}$ が正しく検出される場合、すなわち、 $y^{\wedge}_{i,j} = y_{i,j}$ の場合、 $q^{\pm}_{i,j} = 0$ となり、第2透かしを完全に除去することが可能である。視覚モデルを用いた場合には、埋め込み時と抽出時においては、スケーリングパラメータを計算する対象の画像は異なるものの、両画像の違いを認知できないほど似通っているため、 $\beta^+_{i,j} \doteq \beta^{\wedge+}_{i,j}$ 、 $\beta^-_{i,j} \doteq \beta^{\wedge-}_{i,j}$ となる。以上により、第2透かしビット $y^{\wedge}_{i,j}$ が正しく検出される場合、すなわち、 $y_{i,j} = y^{\wedge}_{i,j}$ の場合、第2透かしの除去により発生したノイズ $q^{\pm}_{i,j}$ はゼロに近似される。

【0097】

(5) 第1透かしの抽出手順

第1透かし抽出ブロック220の第1抽出部48による第1透かしの抽出手順を説明する。第1抽出部48は、第2透かし抽出ブロック210から第2透かし Y^{\wedge} が除去された第1埋め込みホスト信号 W^{\wedge} を受け取り、第1透かしビット x

i を検出するために、次の検出値 z_i を計算する。

$$\begin{aligned} z_i &= \sum_{j=0}^{m_1-1} (w^{+}_{i,j} - w^{-}_{i,j}) \\ &= \sum_{j=0}^{m_1-1} [(v^{+}_{i,j} - v^{-}_{i,j}) + (\alpha^{+}_{i,j} + \alpha^{-}_{i,j}) \cdot x_i + (q^{+}_{i,j} + q^{-}_{i,j}) + (n^{+}_{i,j} - n^{-}_{i,j})] \end{aligned}$$

ただし、 $q^{\pm}_{i,j}$ は、元のホストデータ $v^{\pm}_{i,j}$ に埋め込まれている第2透かしビットの除去後に生じたノイズである。また、 $n^{\pm}_{i,j}$ は、信号処理などにより、元のホストデータ $v^{\pm}_{i,j}$ に加えられたノイズを示す。

【0098】

ここで $\sum_{j=0}^{m_1-1} (v^{+}_{i,j} - v^{-}_{i,j})$ は m_1 が十分に大きいとき、一般にガウス分布に従い、0 に近づく。ノイズの項 $\sum_{j=0}^{m_1-1} (n^{+}_{i,j} - n^{-}_{i,j})$ についても同様に0に近づく。 $\sum_{j=0}^{m_1-1} (q^{+}_{i,j} + q^{-}_{i,j})$ の項についても、第2透かしが正しく抽出されている場合には、0に近似できる。したがって、検出値 z_i は $\sum_{j=0}^{m_1-1} [(\alpha^{+}_{i,j} + \alpha^{-}_{i,j}) \cdot x_i]$ の値で近似できる。 $(\alpha^{+}_{i,j} + \alpha^{-}_{i,j})$ は正であるから、第1透かしビット x_i が1ならば z_i は正であり、第1透かしビット x_i が-1ならば z_i は負である。したがって z_i の正負により第1透かしビット x_i の値を判定することができる。

【0099】

以上のことより、検出値 z_i は、次式のように近似される。

$$\begin{aligned} z_i &= \sum_{j=0}^{m_1-1} (w^{+}_{i,j} - w^{-}_{i,j}) \\ &\doteq \sum_{j=0}^{m_1-1} [(v^{+}_{i,j} - v^{-}_{i,j}) + (\alpha^{+}_{i,j} + \alpha^{-}_{i,j}) \cdot x_i] \end{aligned}$$

【0100】

第1透かし抽出ブロック220の第1抽出部48は、第1埋め込みホスト信号 W^{\wedge} を受け取り、検出値 z_i を計算した後、ECC復号部45が硬入力 of 復号器で構成される場合には、検出値 z_i の正負で、第1透かしビット x_i^{\wedge} が $\{-1, 1\}$ のいずれであるかを判定し、第1透かしデータ X^{\wedge} を得る。また、ECC復号部45が軟入力 of 復号器で構成される場合には、検出値 z_i を $\{-1, 1\}$

に硬判定することなく、そのまま、ECC復号部45に送る。

【0101】

抽出された第1透かしデータ X^{\wedge} はさらにECC復号部45により誤り訂正がなされて出力される。

【0102】

(6) 透かしベクトルの許容劣化領域

図15は、GS方式によるホストデータVに対する透かしビット系列の候補を説明する図である。透かし埋め込み対象のホストデータ v をホストデータの信号空間のある1点であるとする、このホストデータ v に対して人間の視覚モデルから決定される知覚上の劣化を生じない非線形領域（以下許容劣化領域300という）が同図のように定まる。ただし、説明の便宜上、信号空間を2次元空間で示している。透かし系列の候補数が16の場合、第1透かしベクトルの候補 $x_0 \sim x_{15}$ がスクランブルにより得られる。これらの第1透かしベクトル候補 x_i （ $i=0, \dots, 15$ ）をホストデータ v に加算する際、許容劣化領域300に収まるようにスケーリングパラメータ α_i を乗算することで透かしの増幅を行う。その結果、16個の第1埋め込みホストデータの候補 w_0, \dots, w_{15} が得られる。これらの候補の中で埋め込み透かしのSN比が最大のものを選択すると、同図の例では、ベクトル長が最大である第1埋め込みホストデータ w_5 が得られる。

【0103】

次に、第2透かしベクトルの候補 y_i （ $i=0, \dots, 15$ ）をスクランブルにより生成して、最適な第1埋め込みホストデータ w_5 に同様に埋め込むと、図16に示すように、最適な第1埋め込みホストデータ w_5 に対して決定される許容劣化領域310内で、16個の第2埋め込みホストデータの候補 u_0, \dots, u_{15} が得られる。これらの候補の中で埋め込み透かしのSN比が最大のものを選択すると、同図のように最適な第2埋め込みホストデータ u_9 が得られる。

【0104】

ここで、最適な第2埋め込みホストデータ u_9 は元のホストデータ v の許容劣

化領域 300 内には収まっていない。このように透かしを多重に埋め込むと、一般には多重埋め込みホストデータは、元のホストデータの許容劣化領域内に収まらないことになる。そこで、図 17 に示すように、ホストデータ v の許容劣化領域 300 と第 1 透かし埋め込み後の最適な第 1 埋め込みホストデータ w_5 に対して決定される許容劣化領域 310 との共通領域 312 内に制限して、第 2 埋め込みホストデータの候補を選択する。共通領域 312 内で埋め込み透かしの SN 比が最大のものを選択すると、同図のように、最適な第 2 埋め込みホストデータ u_{11} が得られ、二重埋め込みホストデータは元のホストデータ v の許容劣化領域 300 内に収まる。多重に透かしを埋め込む場合も同様の制限を行い、多重埋め込みホストデータが元のホストデータ v の許容劣化領域 300 内に収まるようにすることができる。

【0105】

第 2 埋め込みホストデータの選択範囲を広げるために、図 18 のように、緩和係数 $A (> 1)$ により、スケーリングパラメータ α を $\alpha \cdot A$ に緩和して、ホストデータ v の許容劣化領域 300 を緩和許容劣化領域 302 に広げてよい。この場合、ホストデータ v の緩和許容劣化領域 302 と最適な第 1 埋め込みホストデータ w_5 に対して決定される許容劣化領域 310 との共通領域 314 内に制限して、第 2 埋め込みホストデータの候補を選択するため、選択対象の候補が増え、ベクトル長がより長い u_{10} が最適な第 2 埋め込みホストデータとして得られる。

【0106】

以下、図 17 および図 18 の第 2 埋め込みホストデータの候補 U^k の選択手順を詳細に述べる。GS 方式により第 1 透かしの埋め込みを行った場合、第 1 埋め込みホストデータ W は次式で与えられる。

$$w^+_{i,j} = v^+_{i,j} + \alpha^+_{i,j} \cdot x^k_{i,j}$$

$$w^-_{i,j} = v^-_{i,j} - \alpha^-_{i,j} \cdot x^k_{i,j}$$

ただし、 $\{v^\pm_{i,j}\}$ ($i=0, \dots, n_1-1, j=0, \dots, m_1-1$) はホストデータ V から秘密鍵 K_1 にもとづいて選択されたサンプル集合である。

【0107】

第2埋め込みホストデータの候補 U^k は次式で与えられる。

$$u^{k+i, j} = w^{+i, j} + \beta^{+i, j} \cdot y^{k, i}$$

$$u^{k-i, j} = w^{-i, j} - \beta^{-i, j} \cdot y^{k, i}$$

ただし、 $\{w^{\pm i, j}\}$ ($i=0, \dots, n_2-1, j=0, \dots, m_2-1$) は第1埋め込みホストデータ W から秘密鍵 K_2 にもとづいて選択されたサンプル集合である。このサンプル集合 $\{w^{\pm i, j}\}$ は、第1透かしデータ X の埋め込み対象として秘密鍵 K_1 にもとづいて選択されたサンプル集合 $\{v^{\pm i, j}\}$ とは異なる集合であり、サンプル集合 $\{v^{\pm i, j}\}$ とは独立に選択される。したがって、第1透かしデータ X の埋め込み式における $w^{\pm i, j}$ とは区別して $w^{\sim \pm i, j}$ と表記している。

【0108】

ここで、 $w^{\sim \pm i, j}$ は元のホストデータの値 $v^{\sim \pm i, j}$ から $\Delta^{\pm i, j}$ だけ変化していることから、

$$u^{k+i, j} = v^{+i, j} + \Delta^{+i, j} + \beta^{+i, j} \cdot y^{k, i}$$

$$u^{k-i, j} = v^{-i, j} - \Delta^{-i, j} - \beta^{-i, j} \cdot y^{k, i}$$

と表すことができる。ここで $\Delta^{\pm i, j}$ の値は、埋め込まれている第1透かしビットの値により、 $+\alpha^{\sim \pm i, j}$ または $-\alpha^{\sim \pm i, j}$ である。もしくは、第1透かしビットがサンプル $v^{\sim \pm i, j}$ に埋め込まれていない場合は、 $\Delta^{\pm i, j} = 0$ となる。なお、 $v^{\sim \pm i, j}$ は秘密鍵 K_2 により決定されたサンプル $w^{\sim \pm i, j}$ と同じ場所に位置する原ホストデータ V のサンプルであり、 $\alpha^{\sim \pm i, j}$ は、その原サンプル $v^{\sim \pm i, j}$ において決定されたスケーリングパラメータである。

【0109】

$(\Delta^{\pm i, j} \pm \beta^{\pm i, j} \cdot y^{k, i})$ の値は、透かしを二重に埋め込んだことによる原サンプル $v^{\sim \pm i, j}$ からの変化量である。一方、 $\alpha^{\sim \pm i, j}$ は、その原サンプル $v^{\sim \pm i, j}$ に対して許容される最大の変化量である。したがって、添え字の集合 C を次のように定義し、 $k \in C$ となる候補について、SN比が最大になるものを選択すればよいことがわかる。

$$\begin{aligned}
 K &= \arg \max_{k \in C} (P_k / \sigma_k^2) \\
 P_k &= \sum_{i=0}^{n_2-1} \mid \sum_{j=0}^{m_2-1} (u+k_i, j - u-k_i, j) \\
 &\mid^2 / n_2 \\
 \sigma_k^2 &= \sum_{i=0}^{n_2-1} \mid \sum_{j=0}^{m_2-1} (u+k_i, j - u-k_i, j) \\
 &- P_k \mid^2 / n_2 \\
 C &= \{c : \mid \Delta^+_{i, j} + \beta^+_{i, j} \cdot y^c_{i, j} \mid \leq \alpha^+_{i, j}, \\
 &\quad \mid \Delta^-_{i, j} - \beta^-_{i, j} \cdot y^c_{i, j} \mid \leq \alpha^-_{i, j}, \\
 &\quad \forall i=0, \dots, n_2-1, \\
 &\quad \forall j=0, \dots, m_2-1 \}
 \end{aligned}$$

【0110】

添え字の集合Cは、第2埋め込みホストデータの候補 U^k のサンプル集合がすべてホストデータVの許容劣化範囲に収まる領域を示しており、この領域内に存在するホストデータ U^k の中からSN比が最大のものが選択される。緩和許容劣化領域に広げる場合は、 $\alpha^+_{i, j}$, $\alpha^-_{i, j}$ をそれぞれ $A \cdot \alpha^+_{i, j}$, $A \cdot \alpha^-_{i, j}$ に置き換えればよい。緩和係数Aの導入により、透かしの耐性を強化できるが、ホストデータVからの劣化は大きくなる。以上の手順を繰り返し適用すれば、ホストデータVを劣化させることなく、複数の透かしを多重に埋め込むことができる。

【0111】

実施の形態4

図19は実施の形態4に係る電子透かし埋め込み装置100の構成を示す。本実施の形態では、透かし情報Iに非重要データと重要データが含まれ、電子透かし埋め込み装置100は、非重要データを第1透かしデータXとして、重要データを第2透かしデータYとしてホストデータVに埋め込む。重要データとは、たとえばコンテンツの識別データなどの保護情報であり、非重要データとは、そのコンテンツに関連するURL (Uniform Resource Locator) などの予備情報である。

【0112】

暗号化部10は、秘密鍵Kを用いて、透かし情報Iに含まれる非重要データと

重要データをそれぞれ第1透かしデータXと第2透かしデータYに暗号化して、それぞれ第1透かし埋め込みブロック110の変更部13と第2透かし埋め込みブロック120の変更部16に入力する。

【0113】

第1透かし埋め込みブロック110の変更部13は、第1透かしデータXをスクランブルして出力し、第1透かし埋め込み部14は、秘密鍵Kを用いて、スクランブルされた第1透かしデータX'をホストデータVに埋め込み、第1埋め込みホストデータWを出力する。

【0114】

第2透かし埋め込みブロック120の変更部16は、第2透かしデータYをスクランブルして出力し、第2透かし埋め込み部18は、秘密鍵Kを用いて、スクランブルされた第2透かしデータY'を第1埋め込みホストデータWに埋め込み、第2埋め込みホストデータUを出力する。

【0115】

一般に、電子透かしの耐性は透かしのデータ量とトレードオフの関係にある。非重要データが暗号化された第1透かしデータXは、データ量を多くする代わりに、弱い耐性でホストデータVに埋め込み、重要データが暗号化された第2透かしデータYは、データ量を少なく抑え、埋め込みの際の冗長度を増加させることで強い耐性をもたせて第1埋め込みホストデータWに埋め込む。

【0116】

第1透かし埋め込みブロック110の変更部13と第1透かし埋め込み部14は協同して、複数のスクランブルされた透かしデータX'を生成し、それぞれをホストデータVに埋め込み、複数の第1埋め込みホストデータWの候補を生成し、それらの候補の一つを選択する機能をもつ。

【0117】

図20は、第1透かし埋め込みブロック110の変更部13および第1透かし埋め込み部14の機能構成図である。この構成は、図7の構成において、マルチプレクサ20に入力される埋め込み位置情報P*を第1透かしデータXに置き換え、第1埋め込みホストデータWに対する埋め込み処理を行う第2埋め込み部2

7をホストデータVに対する埋め込み処理を行う第1埋め込み部26に置き換えたものである。

【0118】

この図20の構成は、第2透かし埋め込みブロック120の変更部16および第2透かし埋め込み部18の機能構成としても用いることができる。その場合、図20において、マルチプレクサ20に入力される第1透かしデータXを第2透かしデータYに置き換え、ホストデータVに対する埋め込み処理を行う第1埋め込み部26を第1埋め込みホストデータWに対する埋め込み処理を行う第2埋め込み部27に置き換えればよい。もっともこの場合、図20の構成を第2透かし埋め込みブロック120で流用することも可能である。すなわち、セクタ30が出力する第1埋め込みホストデータWを第1埋め込み部26にフィードバックして入力として与え、マルチプレクサ20に第2透かしデータYを入力すれば、第2透かし埋め込みブロック120の動作をなすことができる。このように構成することにより、第1透かし埋め込みブロック110と第2透かし埋め込みブロック120の機能を実質的に同一の構成で実現して、ハードウェアまたはソフトウェアの構成を簡略にすることができる。

【0119】

図21は、実施の形態4に係る電子透かし抽出装置200の構成を示す。図21の第2透かし抽出ブロック210の構成と動作は、図8の第2透かし抽出ブロック210と同様であるが、デスクランブラ46が出力する第2透かしデータYは、第1透かし抽出ブロック220の第1抽出部48には供給されずに、そのまま電子透かし抽出装置200から出力される。

【0120】

図21の第1透かし抽出ブロック220の第1抽出部48とECC復号部45は、それぞれ図8の第1透かし抽出ブロック220の第1抽出部48とECC復号部45と同様の動作を行うが、図21の第1透かし抽出ブロック220の第1抽出部48は第1透かしデータの埋め込み位置情報を利用しない点が異なる。また、図21の第1透かし抽出ブロック220では、ECC復号部45の出力する第1透かしデータ $X^{\wedge}b$ のスクランブルを解除し、先頭部の初期データを取り除

いて第1透かしデータ X^{\wedge} を出力する。

【0121】

第1透かし抽出ブロック220の第1抽出部48、ECC復号部45、およびデスクランブラ47の機能は、第2透かし抽出ブロック210の第2抽出部40、ECC復号部44、およびデスクランブラ46を流用して実現することもできる。すなわち、第2透かし除去部42から出力される第2透かしが除去された第1埋め込みホスト信号 W^{\wedge} をフィードバックして第2抽出部40の入力として与えれば、第1透かし抽出ブロック220の機能を実現することができ、構成を簡略化することができる。

【0122】

第1透かしデータ X は第2透かしデータ Y に比べて、データ量が多く、耐性が弱いため、第2埋め込みホストデータ U に比較的弱いノイズが加えられた場合は、第1透かしデータ X と第2透かしデータ Y がともに正しく検出されるが、強いノイズが加えられた場合は、耐性の弱い第1透かしデータ X は壊れる。しかし、耐性の強い第2透かしデータ Y は正しく検出されるので、重要データをノイズが強い場合でも検出することができるようになる。

【0123】

また、先に埋め込まれる第1透かしデータ X の方が第2透かしデータ Y よりも強い耐性をもつようにしてもよい。ただし、第1透かしデータ X は、可逆埋め込み方式により埋め込まれるものとする。すなわち、埋め込みの順序を逆にして、先に重要データを含む第1透かしデータ X を強い耐性で埋め込み、非重要データをその後に埋め込むことも可能である。この場合、抽出側では、最初に耐性の強い重要データに関する第1透かしデータ X を抽出して、抽出したビットを用いて埋め込みの逆演算を行い、第2透かしデータ Y との干渉を除去する。その後、第2透かしデータ Y を抽出する。第1透かしデータ X と第2透かしデータ Y は互いに干渉しないため、必ずしも埋め込まれた順序と逆の順に透かしを抽出する必要はない。

【0124】

以上述べたように、実施の形態によれば、電子透かしを埋め込む対象となるメ

ディアデータが与えられると、そのメディアデータに応じて、透かしデータを埋め込み易い位置を検出して、透かしを埋め込むことができ、埋め込まれる透かしの耐性を強化することができる。また、GS方式を用いて、透かしビット系列をそのメディアデータに埋め込みやすいビット系列に変換した上で埋め込むことができる。したがって信号処理、幾何変換、圧縮、データの改ざんなどに対する電子透かしの耐性を強化することができ、透かしの検出精度が大幅に改善する。

【0125】

また、透かしが多重に埋め込まれたメディアデータに対して、透かしを順次抽出する際、先に抽出した透かしデータをメディアデータから完全に除去した後に、次の透かしデータを抽出するため、複数の透かしの干渉による誤検出を防ぐことができる。

【0126】

以上、本発明を実施の形態をもとに説明した。これらの実施の形態は例示であり、それらの各構成要素や各処理プロセスの組み合わせにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0127】

そのような変形例として、実施の形態1の実透かし埋め込み部112およびメタ透かし埋め込み部122に、それぞれ実施の形態4の第1透かし埋め込みブロック110および第2透かし埋め込みブロック120の機能構成を利用して、GS方式で実透かしとメタ透かしの埋め込みを行うようにしてもよい。また実施の形態2の実透かし埋め込み部112および第2透かし埋め込み部124に、それぞれ実施の形態3の第1透かし埋め込みブロック110および第2透かし埋め込みブロック120の機能構成を利用して、埋め込み位置情報をGS方式でスクランブルするようにしてもよい。

【0128】

複数の透かしデータの候補を生成するために、多様性に富んだ候補の生成が可能なGS方式を用いたが、他のスクランブル方式を適用してもよく、また何らかの方法でランダムに候補のデータを生成してもよい。また実施の形態では、逆ス

クランブルにより、抽出された透かしデータから元の透かしデータを再現したが、複数種類のスクランブルされた透かしデータと元の透かしデータとを対応づけたテーブルを備え、このテーブルを参照して元の透かしデータを求めてもよい。

【0129】

またスクランブルの際に初期データとして使用した識別データは、透かしデータの先頭に挿入されて復号側に提供されていたが、この識別データを透かしには埋め込まずに、符号化側で秘密鍵として保持、管理してもよい。その場合、復号側はこの秘密鍵を取得した上で、透かしデータのスクランブルを解除する。あるいは、識別データを新たな透かしデータとして、ホストデータに埋め込んでもよい。

【0130】

上記のいずれの実施の形態においても、第1透かしの埋め込み後に第2透かしを埋め込む構成を説明したが、埋め込み順序を逆にして、第1透かしを埋め込む前に第2透かしを埋め込み、第2透かし埋め込み後のホストデータに第1透かしを埋め込んでもよい。第1透かしの埋め込み位置情報を第2透かしとして埋め込む場合であっても、第1透かしの埋め込み位置を先に決定し、第1透かしは埋め込まずにいったんメモリに記憶しておく。そして、第1透かしの埋め込み位置情報を第2透かしとして先にホストデータに埋め込み、その後メモリから第1透かしのデータを読み出して、第1透かしをホストデータに埋め込む。この場合、第2透かし埋め込みブロック120による第2透かし埋め込み後のホストデータの出力が第1透かし埋め込みブロック110に埋め込み対象のホストデータとして入力される構成にすればよい。

【発明の効果】

本発明によれば、電子透かしの耐性が向上し、透かしの検出精度が改善する。

【図面の簡単な説明】

【図1】 実施の形態1に係る電子透かし埋め込み装置の構成図である。

【図2】 実施の形態1に係る電子透かし抽出装置の構成図である。

【図3】 実施の形態2に係る電子透かし埋め込み装置の構成図である。

【図4】 実施の形態2に係る電子透かし抽出装置の構成図である。

【図 5】 実施の形態 3 に係る電子透かし埋め込み装置の構成図である。

【図 6】 図 5 の第 1 透かし埋め込みブロックの機能構成図である。

【図 7】 図 5 の第 2 透かし埋め込みブロックの機能構成図である。

【図 8】 実施の形態 3 に係る電子透かし抽出装置の構成図である。

【図 9】 図 6 の第 1 透かし埋め込みブロックによる第 1 透かしデータの埋め込み手順を説明するフローチャートである。

【図 10】 第 2 透かしデータとスクランブルされた第 2 透かしデータとの関係を説明する図である。

【図 11】 透かし埋め込み時の畳み込み演算を説明する図である。

【図 12】 透かし抽出時の畳み込み演算を説明する図である。

【図 13】 図 13 (a)、(b) は、スクランブルされた透かしデータの埋め込み方法を説明する図である。

【図 14】 図 7 の第 2 透かし埋め込みブロックによる第 2 透かしデータの埋め込み手順を説明するフローチャートである。

【図 15】 第 1 透かしベクトルの候補の空間を説明する概念図である。

【図 16】 第 2 透かしベクトルの候補の空間を説明する概念図である。

【図 17】 第 2 透かしベクトルの最適な選択例を説明する図である。

【図 18】 第 2 透かしベクトルの別の最適な選択例を説明する図である。

【図 19】 実施の形態 4 に係る電子透かし埋め込み装置の構成図である。

【図 20】 図 19 の第 1 透かし埋め込みブロックの機能構成図である。

【図 21】 実施の形態 4 に係る電子透かし抽出装置の構成図である。

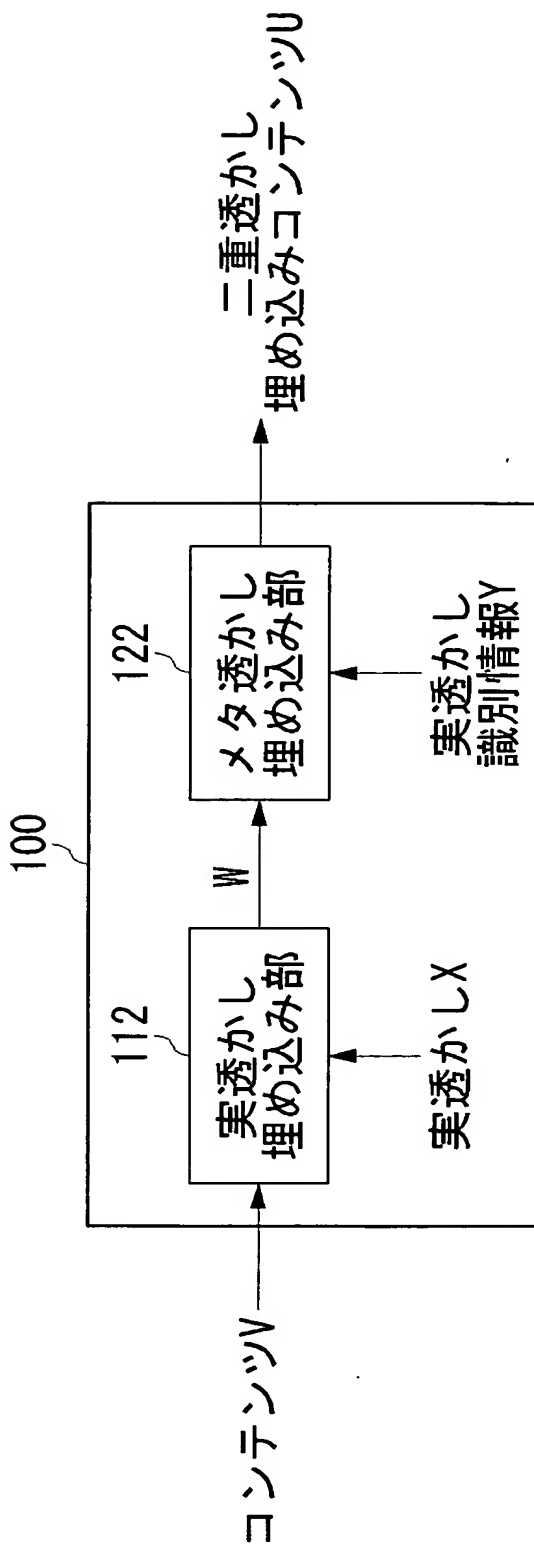
【符号の説明】

10 暗号化部、 12 位置検出部、 14 第 1 透かし埋め込み部、 16 変更部、 18 第 2 透かし埋め込み部、 20 マルチプレクサ、 22 スクランブラ、 24 ECC 部、 26 第 1 埋め込み部、 27 第 2 埋め込み部、 28 SNR 計算部、 30 セレクタ、 40 第 2 抽出部、 42 第 2 透かし除去部、 44 ECC 復号部、 46 デスクランブラ、 48 第 1 抽出部、 60 位置情報生成部、 100 電子透かし埋め込み装置、 110 第 1 透かし埋め込みブロック、 120 第 2 透かし埋め込みブ

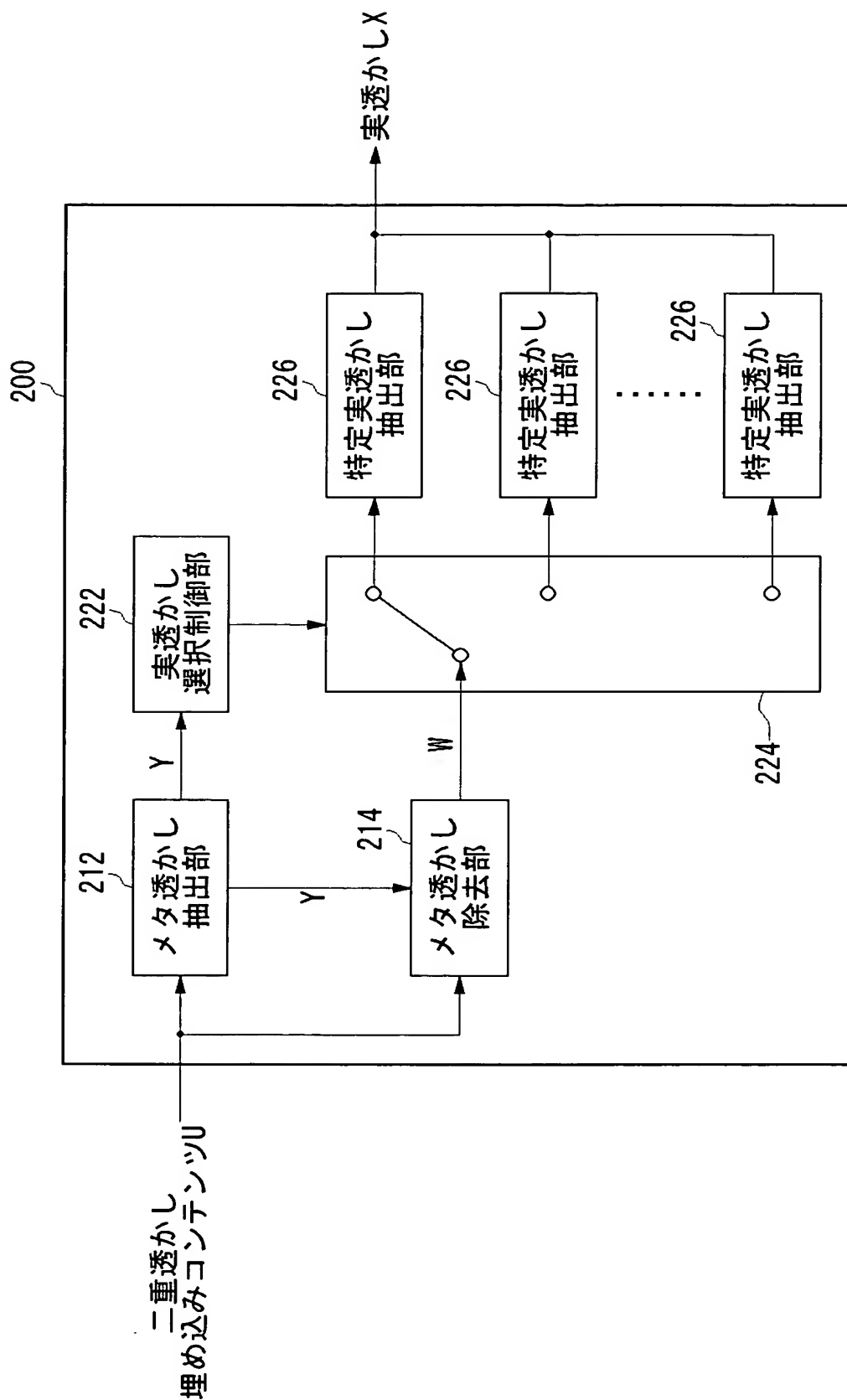
ロック、 2 0 0 電子透かし抽出装置、 2 1 0 第 2 透かし抽出ブロック、
2 2 0 第 1 透かし抽出ブロック。

【書類名】 図面

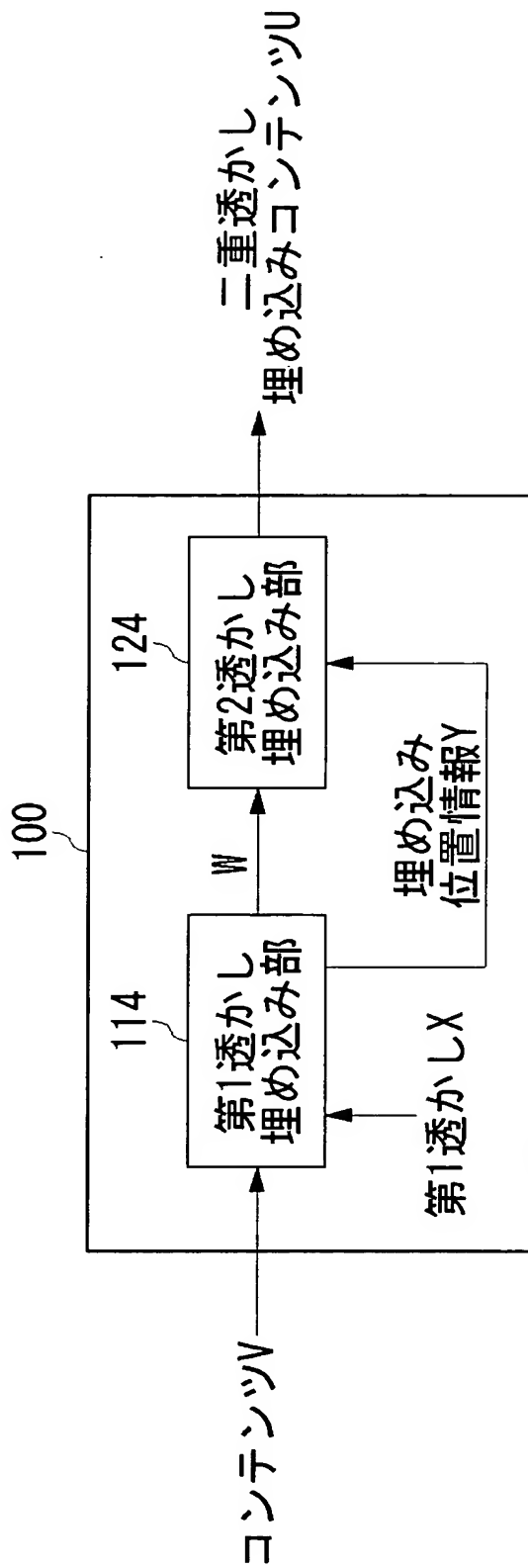
【図 1】



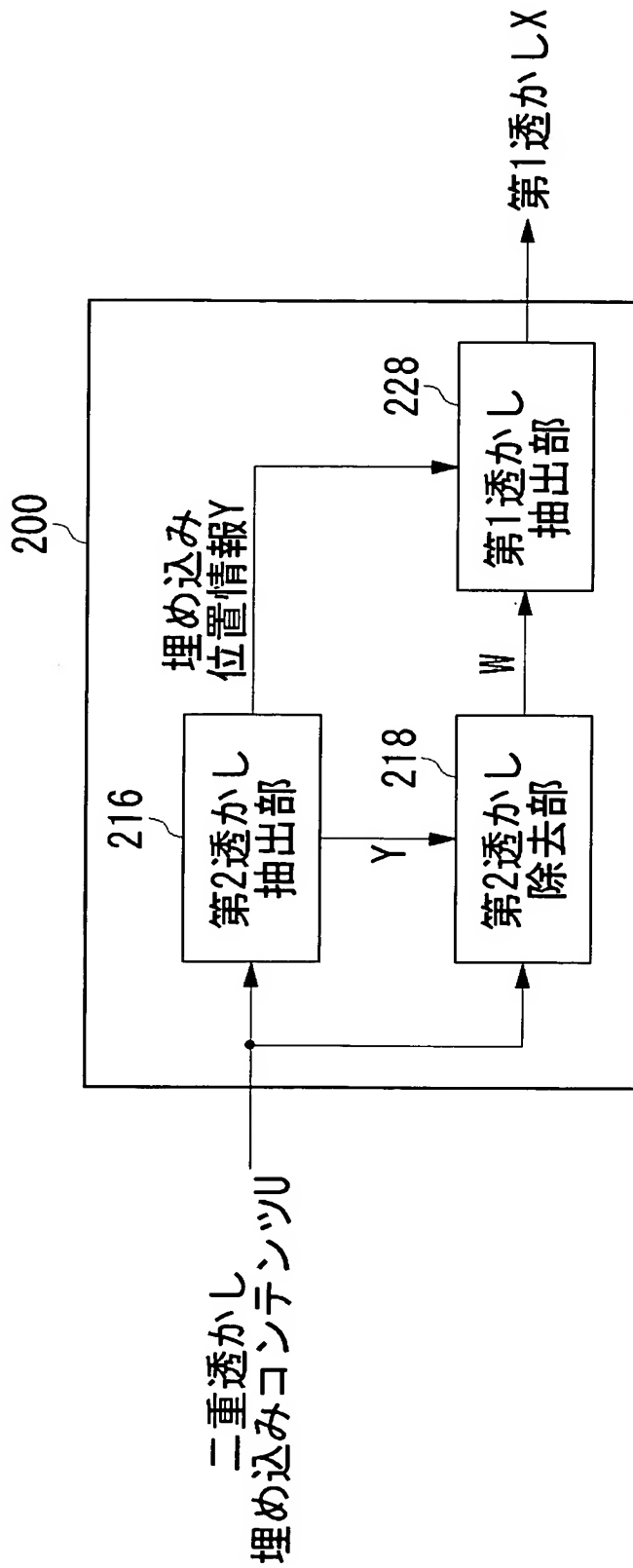
【図 2】



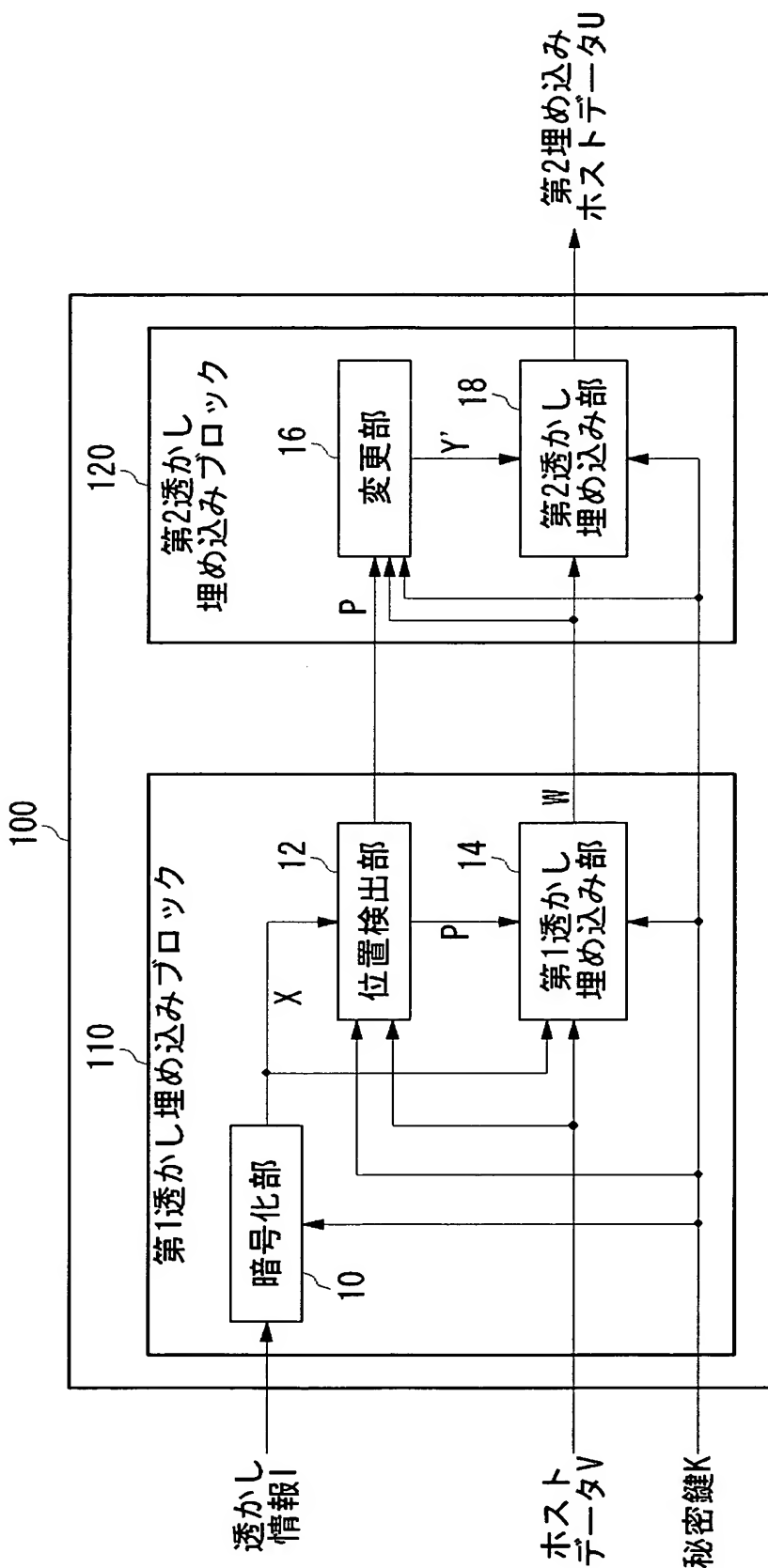
【図 3】



【図 4】

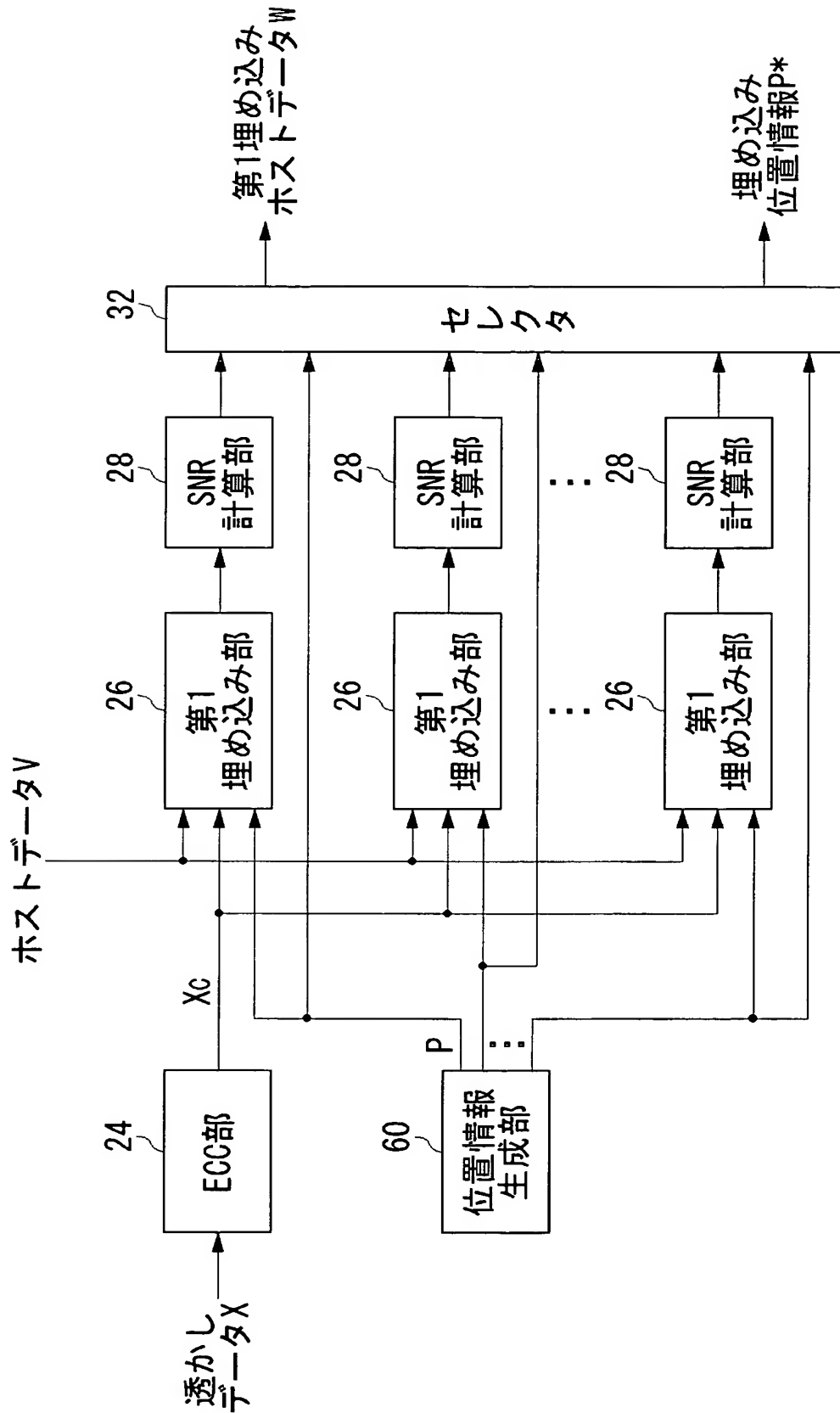


【図 5】

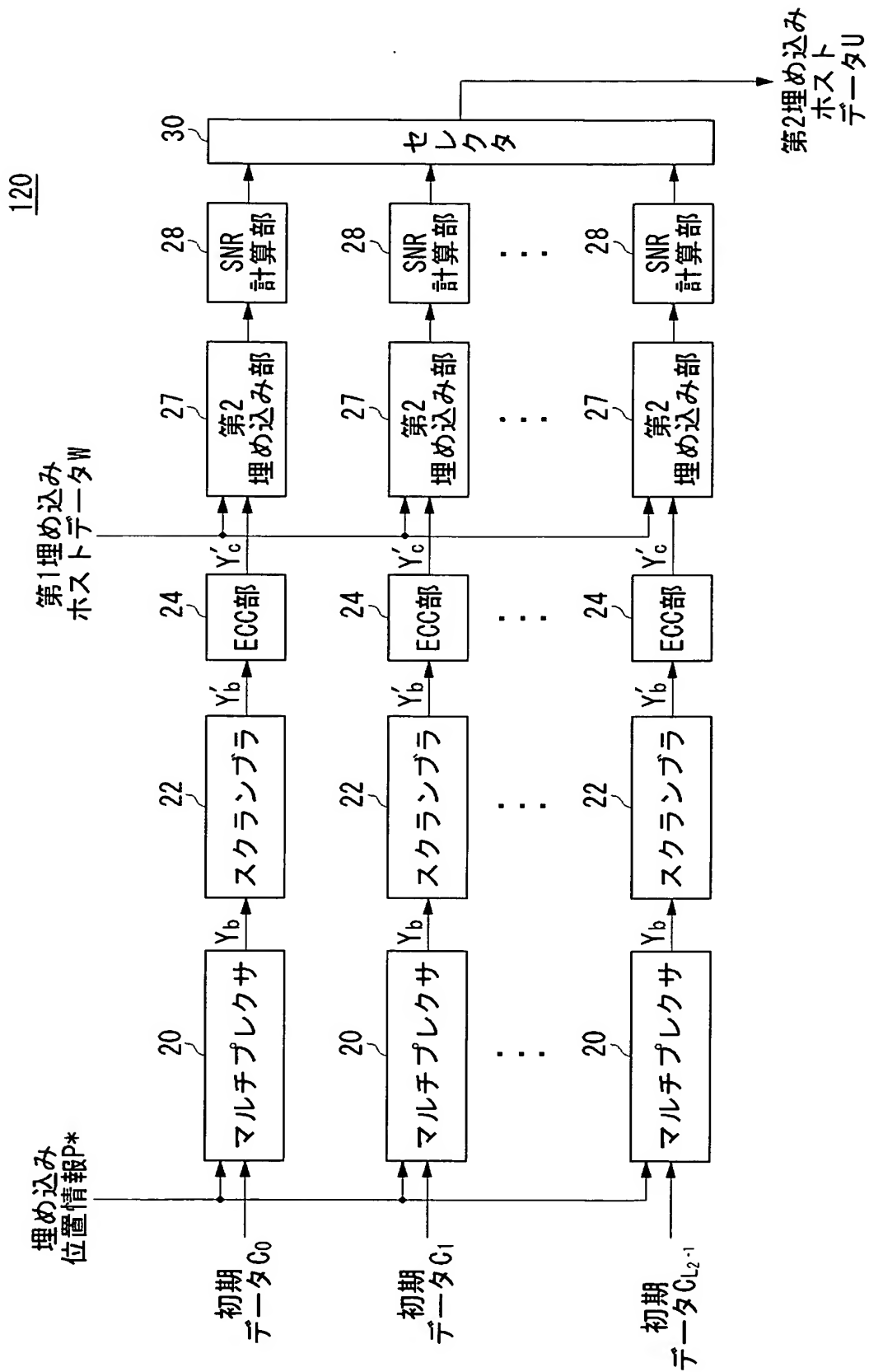


【図 6】

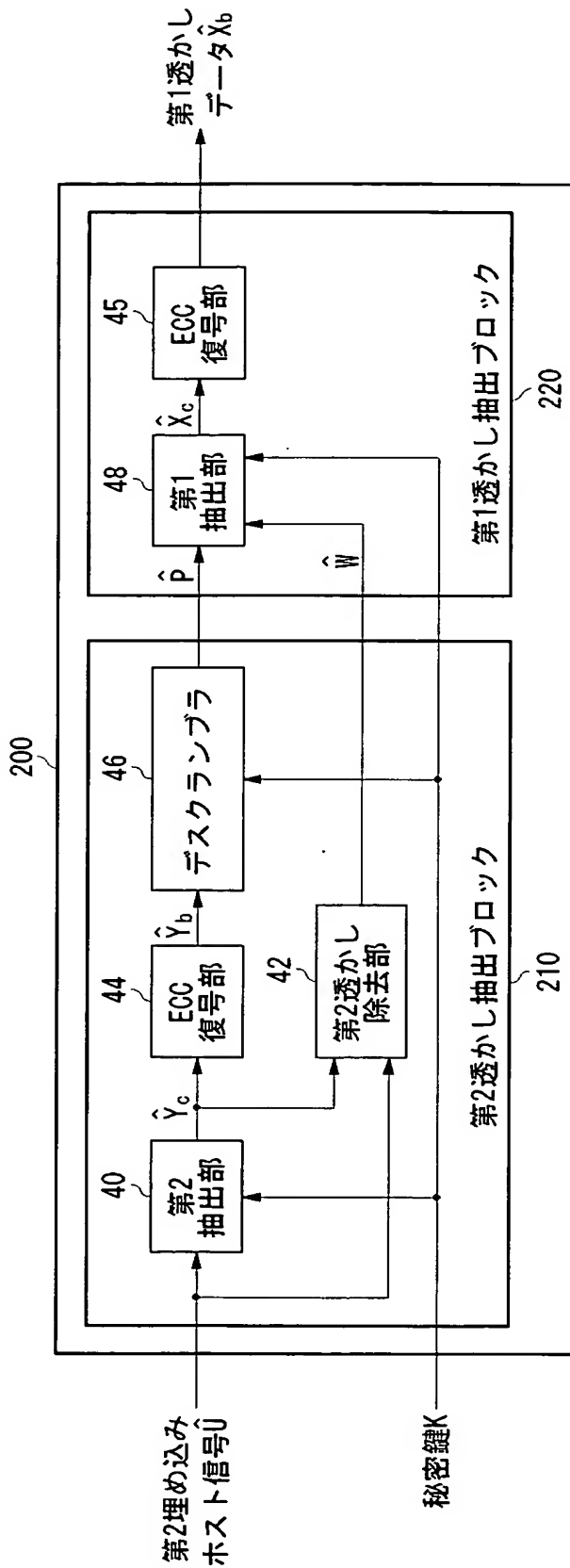
110



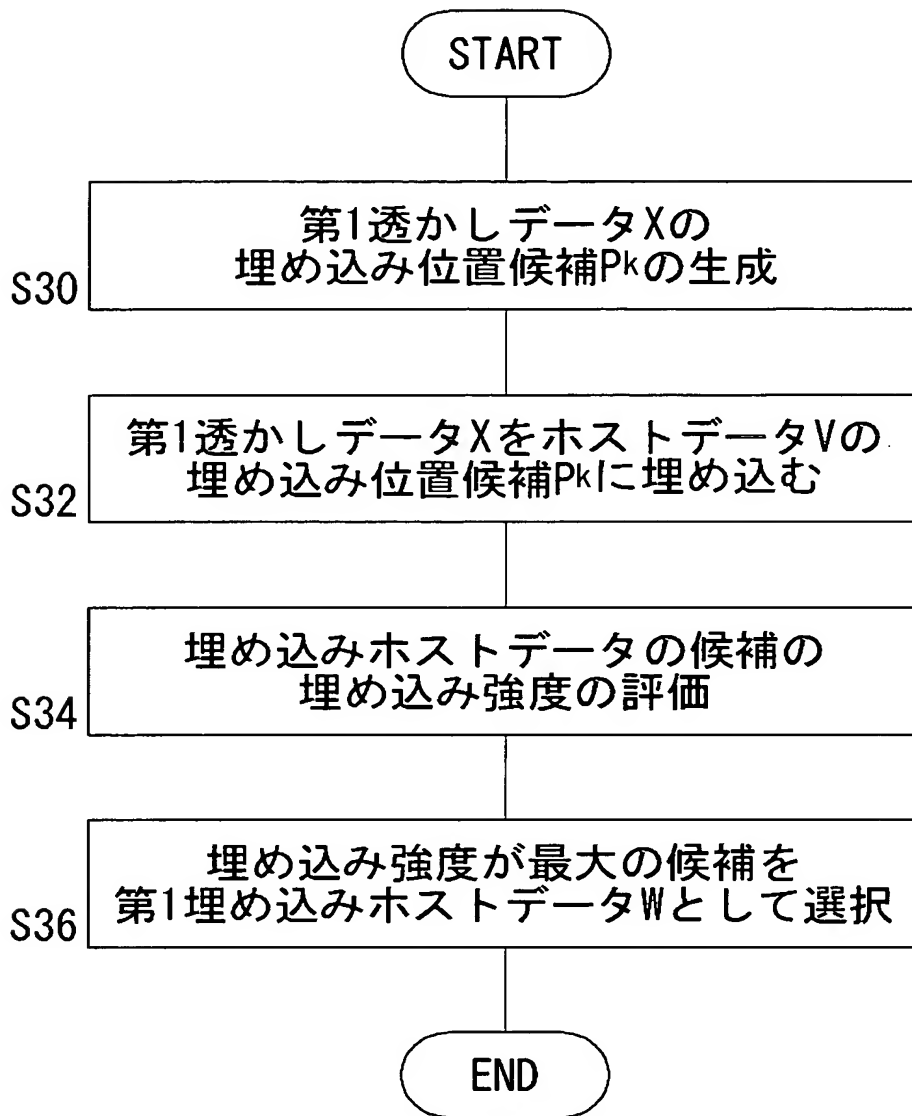
【図 7】



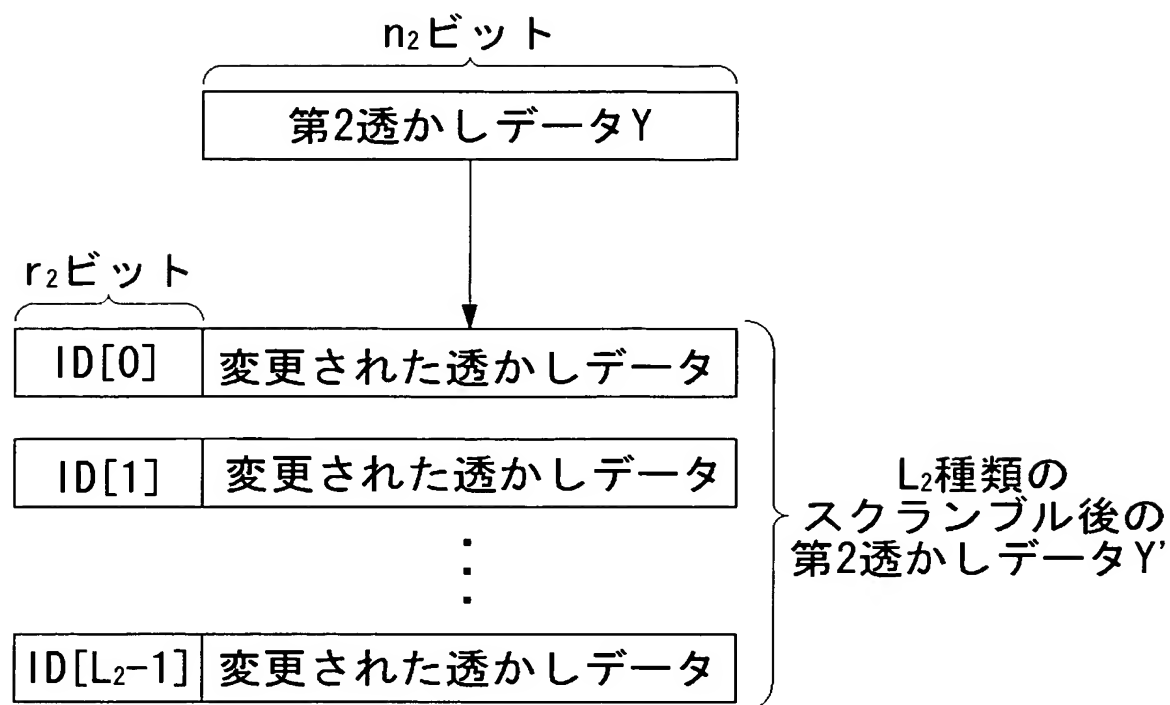
【図 8】



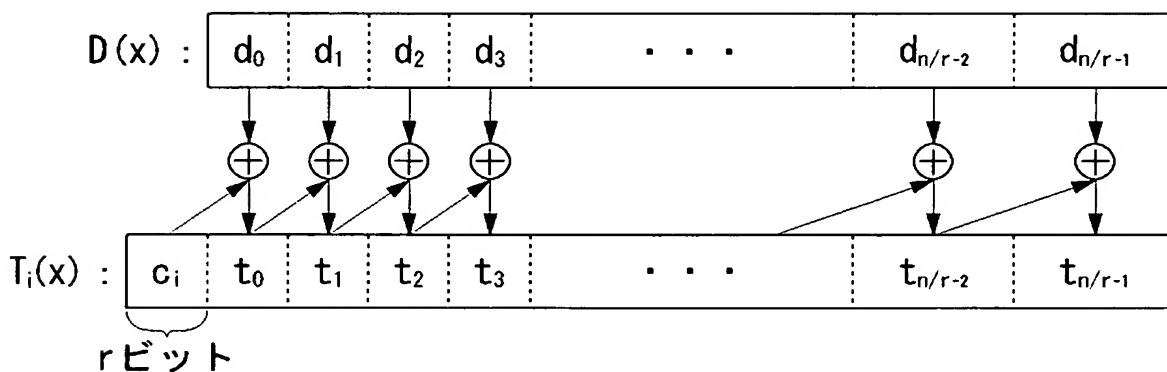
【図 9】



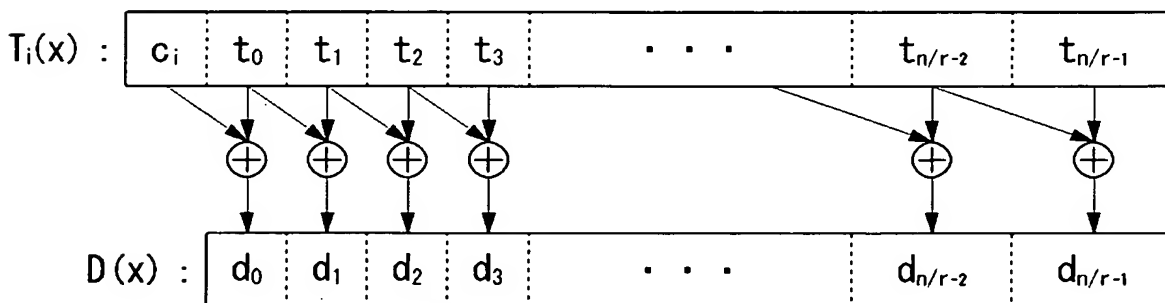
【図 10】



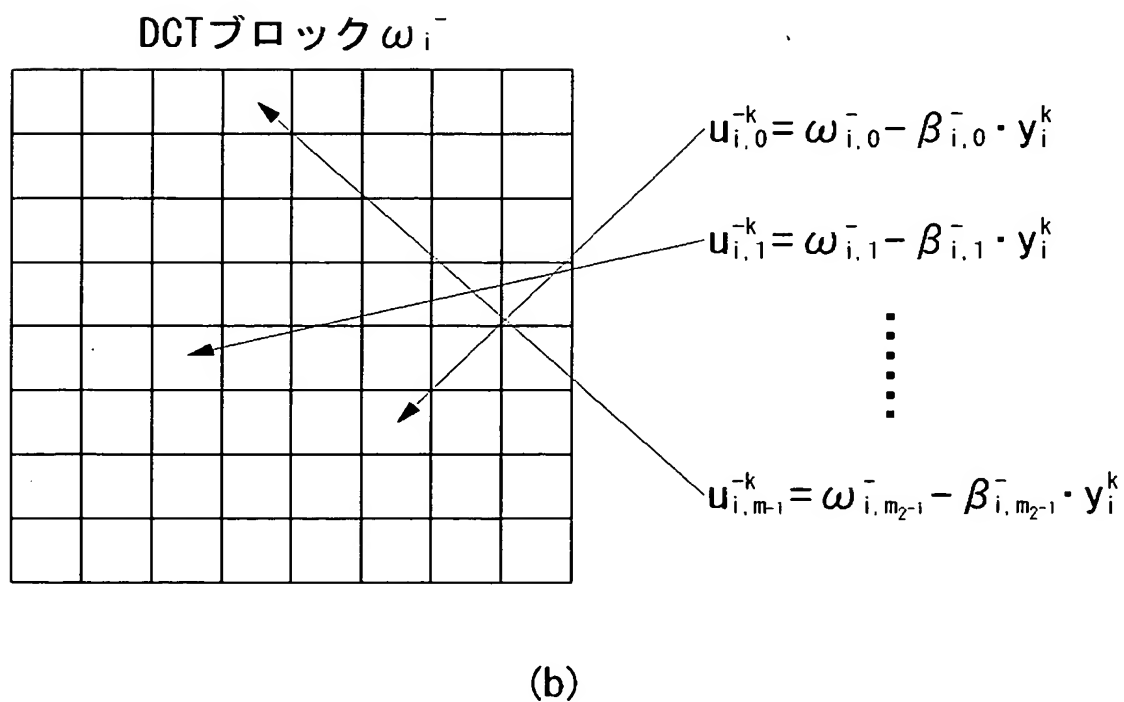
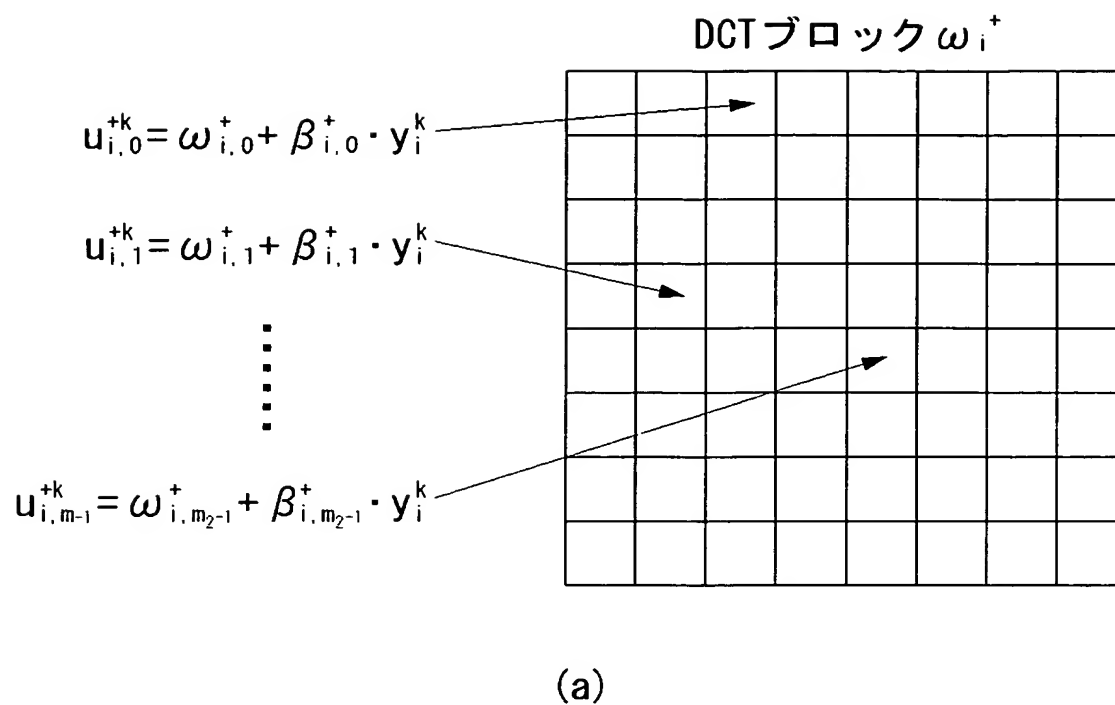
【図 11】



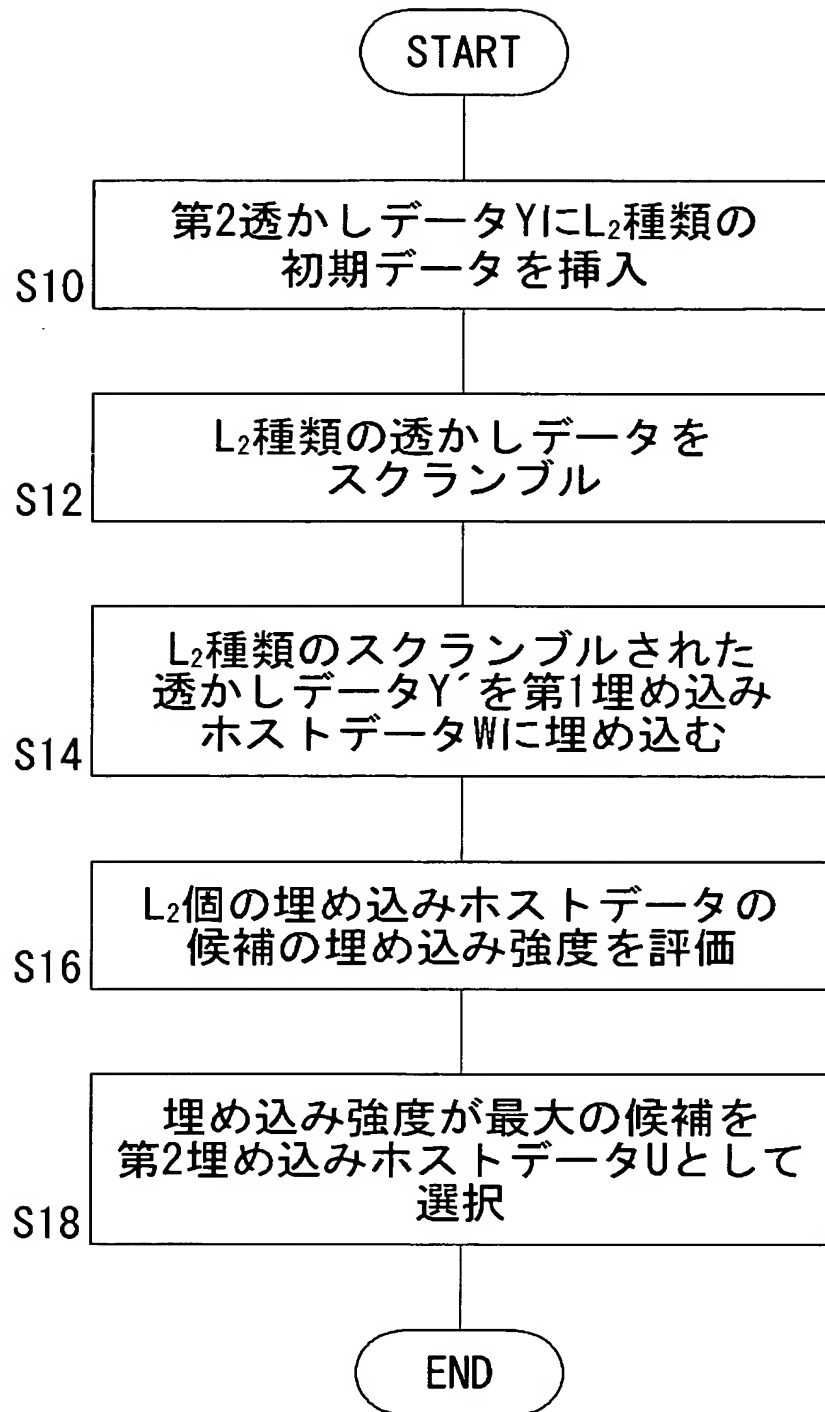
【図 12】



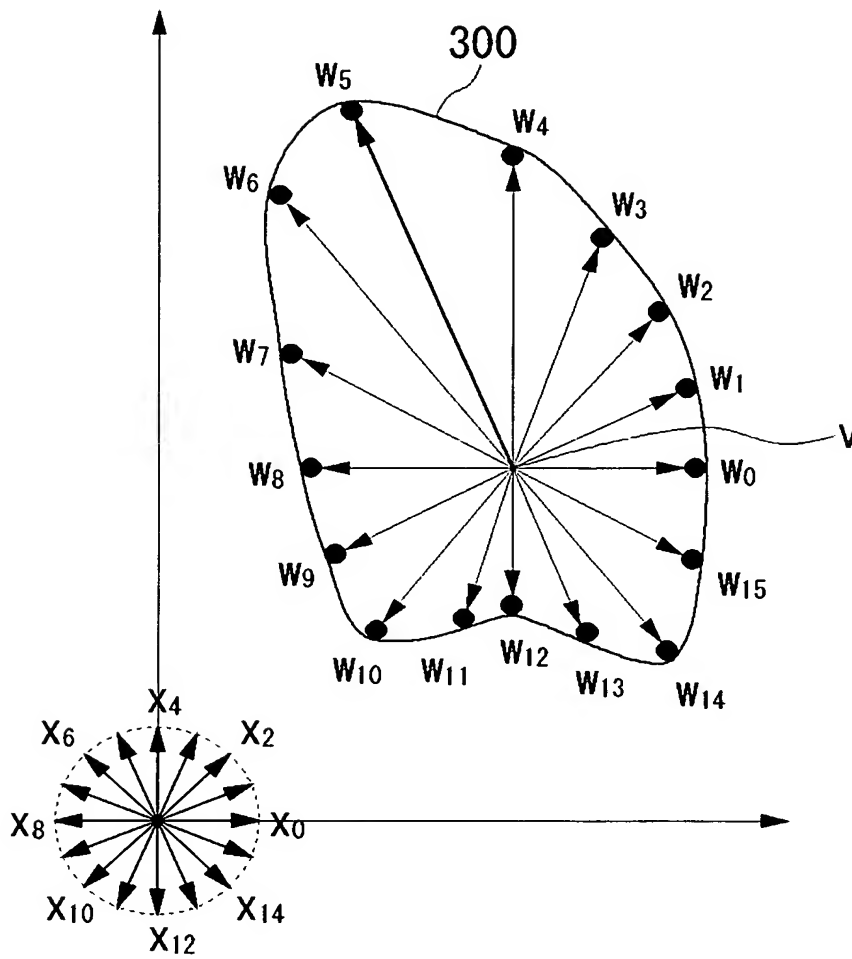
【図 13】



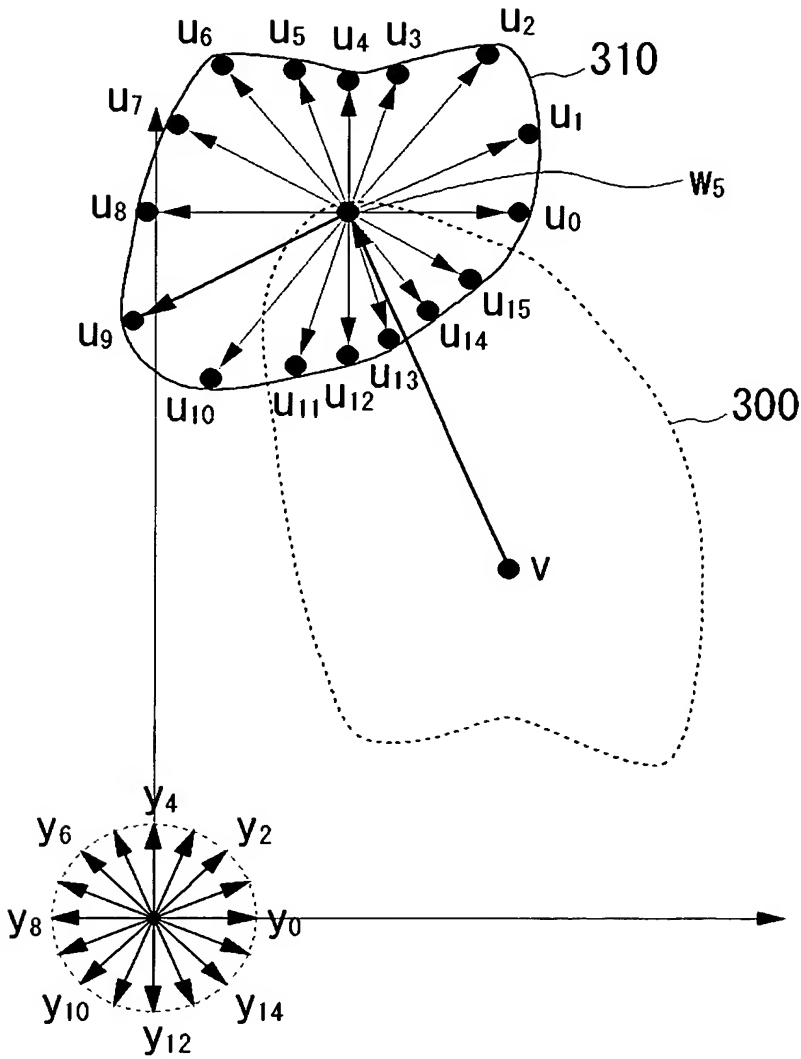
【図 14】



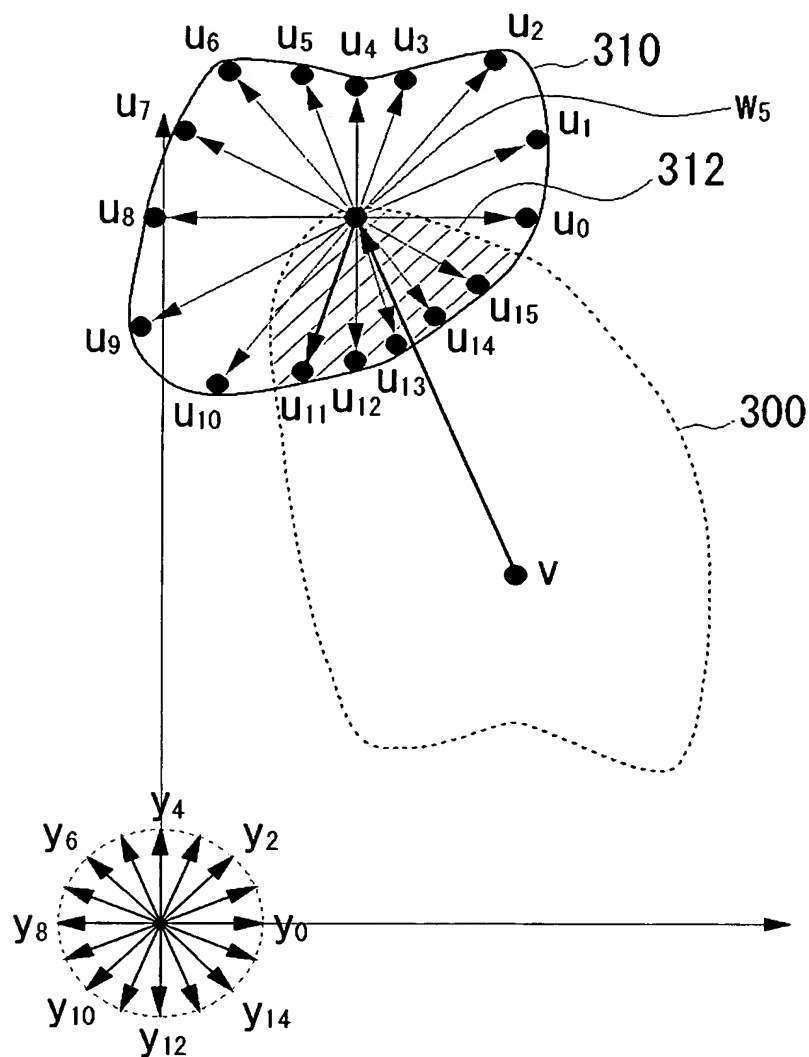
【図 15】



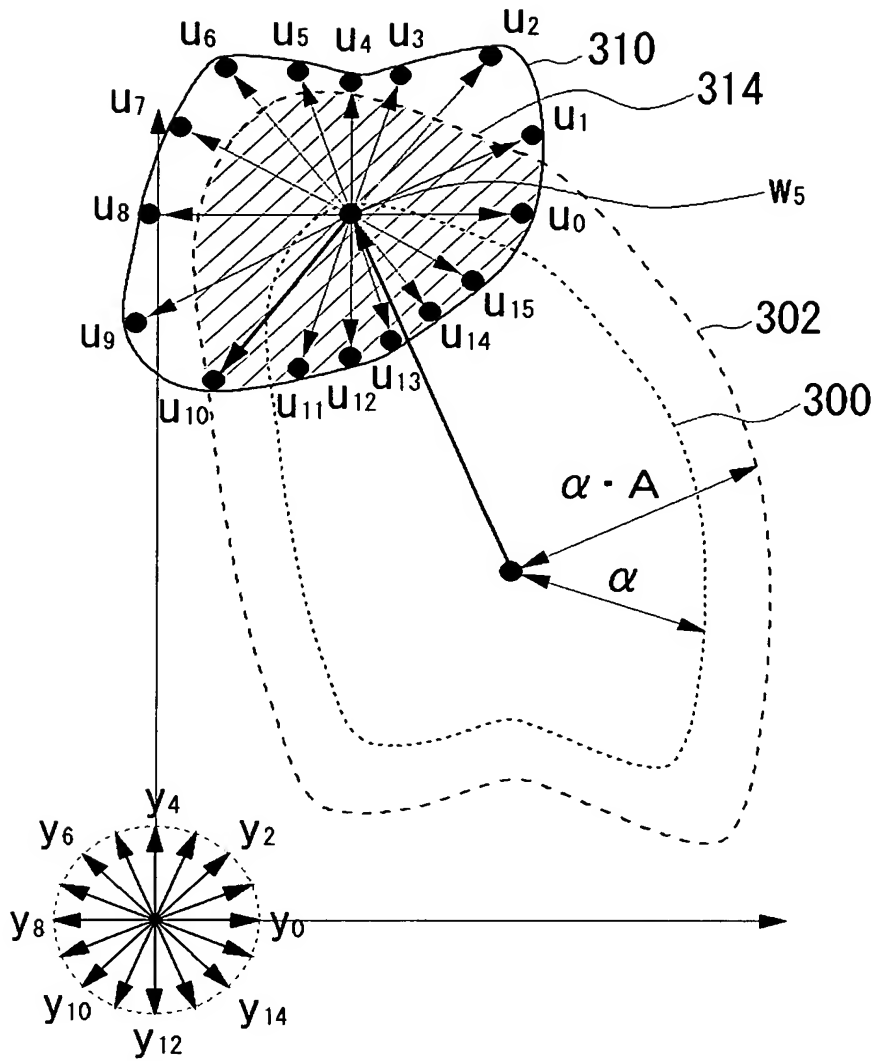
【図 16】



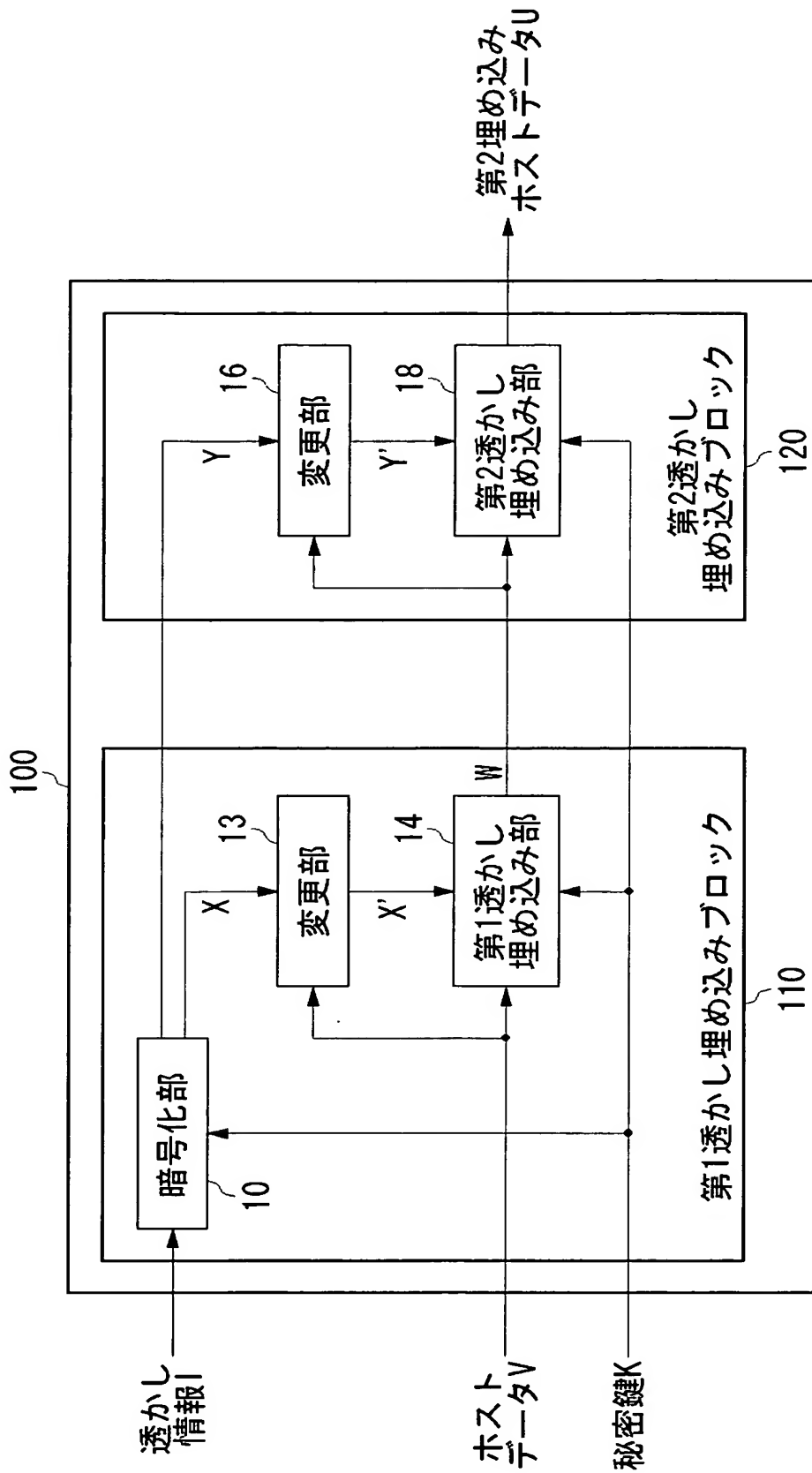
【図 17】



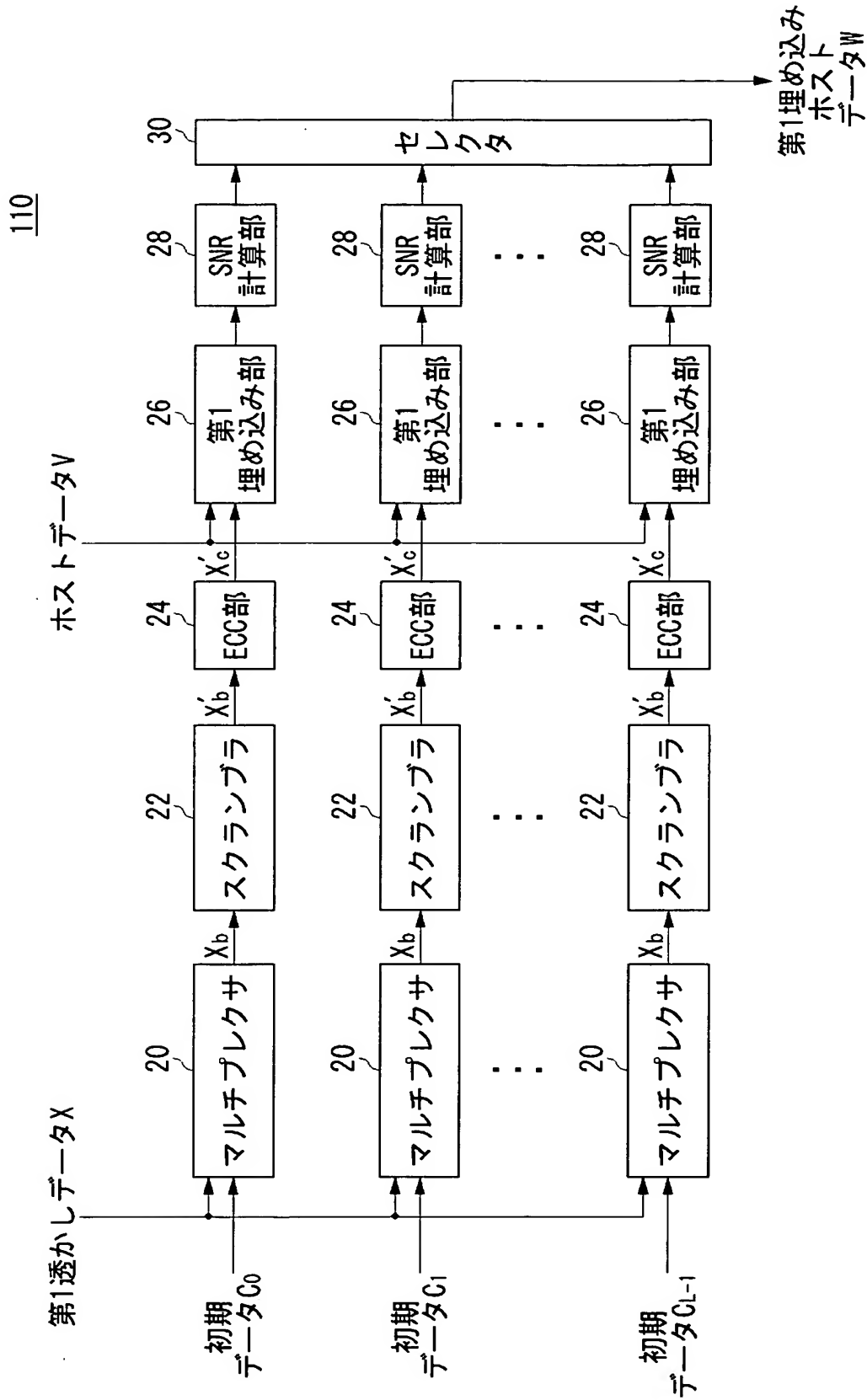
【図 18】



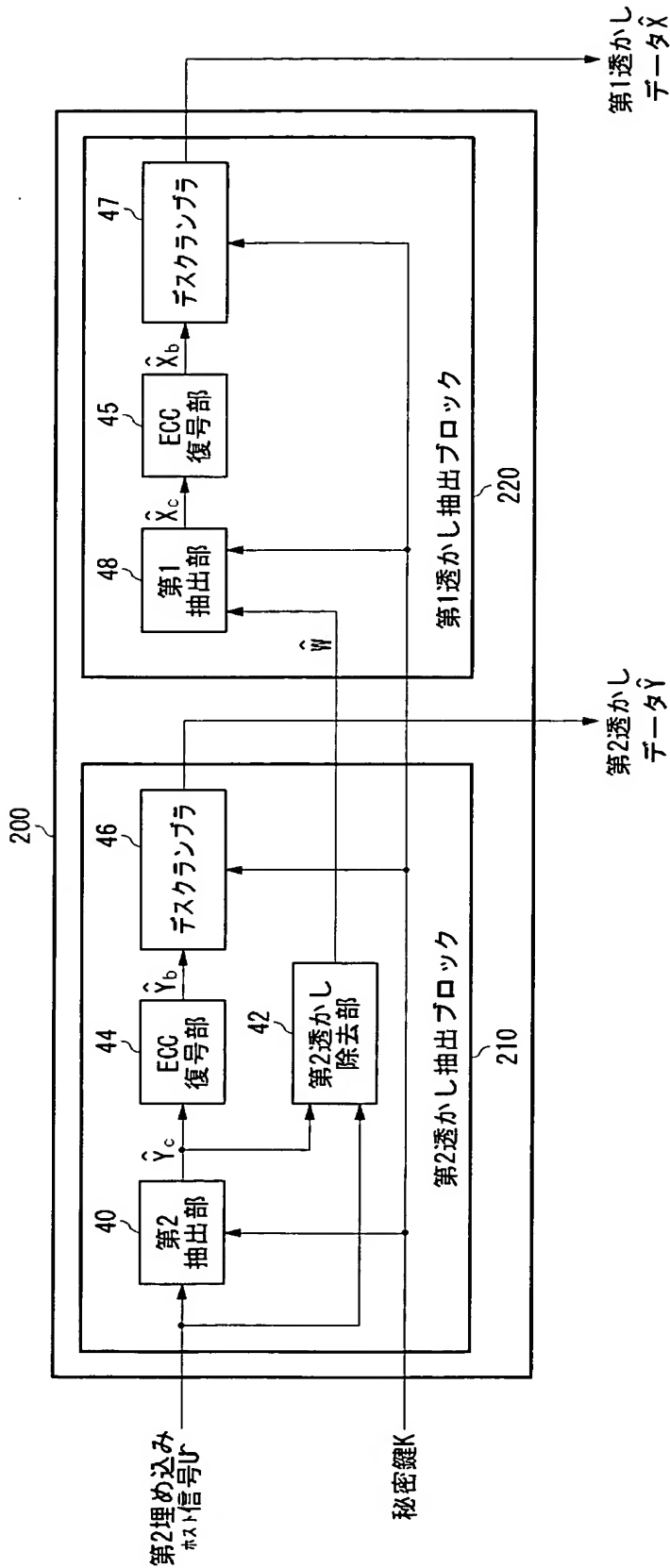
【図 19】



【図 20】



【図 21】



【書類名】 要約書

【要約】

【課題】 電子透かしの耐性を強化し、透かしの検出精度を改善するのは難しい。

【解決手段】 第1透かし埋め込みブロック110において、位置検出部12は、第1透かしデータXの複数の埋め込み位置Pの候補を生成し、第1透かし埋め込み部14は、ホストデータVのそれらの埋め込み位置Pの候補に第1透かしデータXを埋め込み、透かしの耐性が強い第1埋め込みホストデータWを選択して出力する。第2透かし埋め込みブロック120において、変更部16は、第1透かしデータXの埋め込み位置Pに関する情報をスクランブルして複数の第2透かしデータY'の候補を生成し、第2透かし埋め込み部18は、それらの候補を第1埋め込みホストデータWに埋め込み、耐性の強い第2埋め込みホストデータUを選択して出力する。

【選択図】 図5

特願 2 0 0 2 - 3 2 5 8 9 6

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 1 8 8 9]

1. 変更年月日 1 9 9 0 年 8 月 2 4 日
 [変更理由] 新規登録
 住 所 大阪府守口市京阪本通 2 丁目 1 8 番地
 氏 名 三洋電機株式会社

2. 変更年月日 1 9 9 3 年 1 0 月 2 0 日
 [変更理由] 住所変更
 住 所 大阪府守口市京阪本通 2 丁目 5 番 5 号
 氏 名 三洋電機株式会社